7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10.R1

Router Configuration Guide

3HE 17553 AAAB TQZZA

Edition: 01

October 2021

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of Contents

List of Tables

List of Figures

1 Preface

1.1 About This Guide

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

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

Note: This manual generically covers Release 21.x content and may contain some content that will be released in later maintenance loads. Please refer to the 7705 SAR 21.x.Rx Software Release Notes, part number 3HE17436000xTQZZA, for information on features supported in each load of the Release 21.x software.

Note: As of Release 21.4, software support for the following hardware has been deprecated:

- 7705 SAR-M 6-port DSL Combination module (3HE05914AA)
- 7705 SAR-M 8-port xDSL module (3HE05577AA)
- 7705 SAR-M GPON module (3HE05126AA)
- 7705 SAR-Wx xDSL variants (3HE07618AA, 3HE07619AA)

These components are no longer recognized in the release.

1.1.1 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. Concepts described in this guide include the following:

- IP router configuration
- IP, MAC, and VLAN filters
- routing policy options

1.1.2 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 a Nokia service agreement, follow this link to contact a Nokia support representative and to access product manuals and documentation updates:

Product Support Portal

2 7705 SAR Router Configuration Process

Table 1 lists the tasks that are required to configure logical IP routing interfaces, Virtual Router Redundancy Protocol (VRRP) parameters, filtering, routing policies, and Cflowd.

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/Description	Chapter
Router configuration	Configure router parameters, including router interface and addresses, ARP, and ICMP	IP Router Configuration
	Configure VRRP parameters	VRRP
Protocol configuration	Configure IP, MAC, and VLAN filters Configure routing policies Configure Cflowd	Filter Policies Route Policies Cflowd
Reference	List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support

3 IP Router Configuration

This chapter provides information about configuring basic router parameters.

Topics in this chapter include:

3.1 Configuring IP Router Parameters

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

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

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

The following router parameters can be configured:

- Interfaces
- IP Addresses
- Internet Protocol Versions
- Router ID
- Autonomous Systems
- DHCP and DHCPv6
- ICMP and ICMPv6
- Static Routes, Dynamic Routes, and ECMP
- IGP-LDP and Static Route-LDP Synchronization
- Bidirectional Forwarding Detection (BFD)
- Seamless BFD
- IP Fast Reroute (FRR)

3.1.1 Interfaces

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

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

3.1.1.1 Network Interface

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

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

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

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

On the 2-port 10GigE (Ethernet) Adapter card/module, the network interface can only be created on the v-port (not the ring ports).

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

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

Some network Ethernet ports support network egress per-VLAN shapers on a per-network-interface basis. Refer to the “Per-VLAN Network Egress Shapers” section in the 7705 SAR Quality of Service Guide for details.

3.1.1.1.1 Ethernet Ports and Multiple ARP Entries

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

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

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

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

3.1.1.1.2 Dynamic ARP and Static MAC entry

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

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

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

Note:

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

3.1.1.1.3 Configurable ARP Retry Timer

A timer is available to configure a shorter retry interval when an ARP request fails. An ARP request may fail for a number of reasons, such as network connectivity issues. By default, the 7705 SAR waits 5000 ms before retrying an ARP request. The configurable retry timer makes it possible to shorten the retry interval to between 100 and 30 000 ms.

Note: The ARP retry default value of 5000 ms is intended to protect CPU cycles on the 7705 SAR, especially when it has a large number of interfaces. Configuring the ARP retry timer to a value shorter than the default should be done only on mission-critical links, such as uplinks or aggregate spoke SDPs transporting mobile traffic; otherwise, the retry interval should be left at the default value.

The configurable ARP retry timer is supported on VPRN and IES service interfaces, as well on the router interface.

3.1.1.1.4 Proxy ARP

Proxy ARP is a technique by which a router on one network responds to ARP requests intended for another node that is physically located on another network. The router effectively pretends to be the destination node by sending an ARP response to the originating node that associates the router's MAC address with the destination node's IP address (acts as a proxy for the destination node). The router then takes responsibility for routing traffic to the real destination.

Proxy ARP simplifies networking schemes because it enables nodes on a subnet to reach remote subnets without the need to configure routing or a default gateway.

The 7705 SAR supports both proxy ARP and local proxy ARP. Local proxy ARP is similar to proxy ARP except that it is used within a subnet; the router responds to all requests for IP addresses within the subnet and forwards all traffic between the hosts in the subnet. Local proxy ARP is used on subnets where hosts are prevented from communicating directly.

Typically, routers support proxy ARP only for directly attached networks. The 7705 SAR supports proxy ARP for all known networks in the routing instance where the virtual interface proxy ARP is configured.

Proxy ARP is supported on:

- the global routing table
- IES service interfaces

- VPRN service interfaces

A typical application for proxy ARP is when hosts in a private subnet need to communicate to host/servers via the public Internet; for example, when using network address translation (NAT). Source NAT can be used for creating connections from inside (private network) to outside (public network). If an arriving IP packet on the 7705 SAR matches the NAT policy rules, an internal mapping is created between the private source IP address/source port and a public source IP address/source port. The public IP address and port are configured in the NAT pool policy.

Proxy ARP is therefore required for Source NAT when the NAT pool uses a range of IP public addresses. The NAT pool public IP address can either be in a different subnet than the public interface or in the same subnet as the public interface. Proxy ARP can be used to respond to ARP requests for an IP address in these NAT pools.

Note: Only remote proxy ARP is applicable for NAT.

In order to support NAT and other edge-like environments, proxy ARP supports policies that allow the provider to:

- configure prefix lists that determine for which target networks proxy ARP will be attempted
- configure prefix lists that determine for which source hosts proxy ARP will be attempted

As an example, when a source NAT pool is configured with a dynamic IP pool with the address range 1.1.1.2 to 1.1.1.254 on the public interface 1.1.1.1, proxy ARP can be used to resolve the ARP request of the NAT pool hosts with the local interface (1.1.1.1) MAC address (remote proxy ARP).

As another example, if a NAT pool of addresses in the range 2.2.2.1 to 2.2.2.100 is configured on the public Layer 3 interface 198.51.100.1, then by enabling remote proxy ARP, the 7705 SAR will respond to ARP requests from hosts 2.2.2.1 to 2.2.2.100. In addition, a route policy with a prefix list can be created and used as a proxy ARP policy for finer granularity of the IP range for which proxy ARP is being used.

For detailed information on NAT, see NAT Security.

3.1.1.1.5 ETH-CFM Support

Ethernet Connectivity Fault Management (ETH-CFM) is defined in the IEEE 802.1ag and ITU Y.1731 standards. ETH-CFM specifies protocols, procedures, and managed objects to support fault management (including discovery and verification of the path), detection, and isolation of a connectivity fault in an Ethernet network.

ETH-CFM requires the configuration of specific entities at the global level and at the Ethernet service level and/or network interface level. Maintenance domains (MDs) and maintenance associations (MAs) are configured at the global level. Maintenance association endpoints (MEPs) are configured at the service level and network interface level.

MEPs that are not service-based are referred to as facility MEPs. A facility MEP is a Down MEP that detects failure conditions for an Ethernet transport network using ETH-CCM and, where appropriate, propagates alarm conditions so that the Epipe services that share this common transport are aware of the failure. The 7705 SAR supports facility MEPs on network interfaces.

Facility MEPs are created in the same way as service MEPs, by configuring the ETH-CFM domain and association. However, the association used to build the facility MEP does not include a bridge identifier, as the facility MEP is not bound to a service. The CLI ensures that a bridge identifier is not configured when the association is applied to a facility MEP.

The following applies to facility MEPs on network interfaces:

- the MEP must be a Down MEP
- the port must be in network mode
- the port must be configured for null or dot1q encapsulation
- the MEP supports all fault management functionality, with the exception of alarm indication signaling (AIS)
- the MEP supports all performance monitoring functionality including synthetic loss measurement (SLM)
- the MEP supports throughput measurement via loopback messaging at wire speed
- received CFM messages are processed only when the VLAN ID, the MAC destination address, and the MEP level matches those of the MEP

Network interface facility MEPs are supported on all network Ethernet ports on the 7705 SAR adapter cards and chassis.

For detailed information on ETH-CFM entities and on ETH-CFM support for services, refer to the 7705 SAR Services Guide, “ETH-CFM (802.1ag and Y.1731)”. For information on running Ethernet OAM tests, refer to the 7705 SAR OAM and Diagnostics Guide, “ETH-CFM (802.1ag and Y.1731)”.

3.1.1.2 System Interface

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

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

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

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

3.1.1.3 Unnumbered Interfaces

Unnumbered interfaces are point-to-point interfaces that are not explicitly configured with a dedicated IP address and subnet; instead, they borrow (or link to) an IP address from another interface on the system (the system IP address, another loopback interface, or any other numbered interface) and use it as the source IP address for packets originating from the interface.

The benefits of using unnumbered interfaces are:

- ISP backhaul can be enabled with a single IP address allocated to the CE nodes (network interface address is coupled with the system IP address)

- nodes can be added to or deleted from a network without address changes—unnumbered interfaces are linked to a centralized IP address and therefore do not require any address change if the nodes are relocated. After a topology change, the ARP table is updated to ensure reachability and the upper layer protocols re-establish the peering sessions.

Unnumbered interfaces are supported on:

- network interfaces
- IES interfaces
- VPRN interfaces

Only IPv4 addresses are supported.

Unnumbered interfaces are supported for the IS-IS and OSPF routing protocols and for MPLS (RSVP-TE and LDP). Refer to the 7705 SAR Routing Protocols Guide, “Unnumbered Interfaces” in the OSPF and IS-IS sections, for more information on IS-IS and OSPF unnumbered interface support. Refer to the 7705 SAR MPLS Guide, “RSVP-TE Support for Unnumbered Interfaces” and “LDP Support for Unnumbered Interfaces”, for more information on MPLS unnumbered support.

This feature is supported via both dynamic and static ARP.

The following ports on the 7705 SAR adapter cards, modules, and fixed platforms support IP unnumbered interfaces:

- any datapath Ethernet port with null, dot1q, or qinq encapsulation (with the exception of the 10GigE port on the 2-port 10GigE (Ethernet) Adapter card)
- v-port on the 2-port 10GigE (Ethernet) Adapter card
- MWA ports on the Packet Microwave Adapter card
- any T1/E1 port (access or network) with ppp encapsulation
- any DS3/E3 port (network) with ppp encapsulation
- any OC3/STM1 port (network) with ppp-auto encapsulation (POS)

Note: Unnumbered interfaces do not support PIM routing or IGMP listener capabilities.

3.1.1.4 Creating an IP Address Range

An IP address range can be reserved for IES or VPRN services by using the **config>router>service-prefix** command. When a service interface is configured, the IP address must be in the range specified in the **service-prefix** command. If the **service-prefix** command is not configured, then no limitation exists.

Addresses in the range of a defined **service-prefix** can be allocated to a network port unless the **exclusive** parameter is specified. Then, the address range is exclusively reserved for services.

When defining a range that is a superset of a previously defined service prefix, the new superset definition will replace the original configuration. For example, if a service prefix exists for 10.10.10.0/24, and a new service prefix is configured as 10.10.0.0/16, then the old address (10.10.10.0/24) will be replaced with the new address (10.10.0.0/16).

When defining a range that is a subset of a previously defined service prefix, the subset will replace the existing superset providing that the addresses used by services are not affected. For example, if a service prefix exists for 10.10.0.0/16, and a new service prefix is configured as 10.10.10.0/24, then the 10.10.0.0/16 entry will be unreserved as long as there no services configured that are using the 10.10.x.x addresses other than 10.10.10.x.

3.1.2 IP Addresses

IP addresses are assigned to system interfaces and to network-facing physical or logical ports. The IP addresses are in the form <*ip-address/prefix-length*> or <*ip-address/subnet mask*>.

IP version 4 (IPv4) addresses are supported on all interfaces except the CWDM/ OADM module. On the 2-port 10GigE (Ethernet) Adapter card and 2-port 10GigE (Ethernet) module, an IPv4 network address is assigned to the v-port only.

IP version 6 (IPv6) addresses are supported on:

- access ports (IES only); for a complete list of cards and ports that support IES IPv6 SAPs, refer to the 7705 SAR Services Guide, “IES for Customer Traffic”
- network ports (null or dot1q encapsulation) on:
  - 2-port 10GigE (Ethernet) Adapter card (v-port only)
  - 8-port Ethernet Adapter card
  - 6-port Ethernet 10Gbps Adapter card

  - 8-port Gigabit Ethernet Adapter card
  - 10-port 1GigE/1-port 10GigE X-Adapter card
  - Packet Microwave Adapter card
  - Ethernet ports on the 7705 SAR-M
  - Ethernet ports on the 7705 SAR-A
  - Ethernet ports on the 7705 SAR-Ax
  - 7705 SAR-W
  - Ethernet ports on the 7705 SAR-Wx
  - 7705 SAR-H
  - Ethernet ports on the 7705 SAR-Hc
  - Ethernet ports on the 7705 SAR-X
  - Ethernet management port
  - 2-port 10GigE (Ethernet) module (v-port only)
  - 4-port SAR-H Fast Ethernet module
  - 6-port SAR-M Ethernet module
- network ports on the 4-port OC3/STM1 Clear Channel Adapter card (POS encapsulation)

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

Network IP addresses can be assigned manually, or assigned dynamically using DHCP when the 7705 SAR is acting as a DHCP client. System IP addresses can be assigned manually, or assigned dynamically using DHCP when the 7705 SAR is acting as a DHCP client and the DHCP server-facing interface is unnumbered. See Unnumbered Interfaces for more information.

3.1.3 Internet Protocol Versions

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

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

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

3.1.3.1 IPv6 Address Format

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

2001:0db8:0a0b:12f0:0000:0000:0000:0001

Note: On the 7705 SAR, any function that displays an IPv6 address or prefix reflects the rules specified in RFC 5952, *A Recommendation for IPv6 Address Text Representation*. Specifically, hexadecimal letters in IPv6 addresses are represented in lowercase, and the correct compression of all leading zeros is displayed.

As per RFC 5952, the above IPv6 address appears as:

2001:db8:a0b:12f0::1

Leading zeros must be omitted from each block in the address. A series of zeros can be replaced with a double colon. The double colon can only be used once in an address.

The IPv6 prefix is the part of the IPv6 address that represents the network identifier. The network identifier appears at the beginning of the IP address and is made up of the network address and subnet address. The IPv6 prefix length, which begins with a forward slash (/), specifies the number of bits in the network identifier; this is similar to the subnet mask in IPv4 addresses. For example, the address 1080:6809:8086:6502::1/64 means that the first 64 bits of the address represent the network identifier; the remaining 64 bits represent the node identifier.

The following adapter cards support the full IPv6 subnet range for IPv6 static routes and interface IP addresses:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card, version 2 and version 3
- 2-port 10GigE (Ethernet) Adapter card (on the v-port)
- 10-port 1GigE/1-port 10GigE X-Adapter card

For these cards, the supported route range for statically provisioned or dynamically learned routes is from /1 to /128. Supported interface IP address prefixes are from /4 to /127, and /128 on system or loopback interfaces.

For all other cards, modules, and ports (including the v-port on the 2-port 10GigE (Ethernet) module), the supported range for statically provisioned or dynamically learned routes is from /1 to /64 or is /128 (indicating a host route). Supported interface IP address prefixes are from /4 to /64, and /128 on system or loopback interfaces.

3.1.3.2 IPv6 Headers

The IPv6 header format is shown in Figure 1. Table 2 describes the fields.

Figure 1 **IPv6 Header Format**

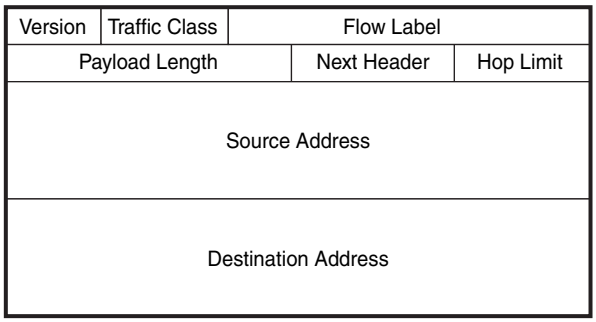


Table 2 **IPv6 Header Field Descriptions**

Field	Description
Version	4-bit IP version number (v6)
Traffic Class	8-bit value that enables a source to identify the delivery classification of its packets
Flow Label	20-bit flow label that can be used by a source to label packets for which the source requests special handling by IPv6 routers; for example, non-default QoS or real-time service A flow contains a series of packets that travel between a particular source and particular destination
Payload Length	The length of the payload (16-bit unsigned integer), which is the rest of the packet following the IPv6 header, in octets Any extension headers that are present in the packet are considered to be part of the payload; therefore, the payload always begins immediately after the Destination Address

Table 2 **IPv6 Header Field Descriptions (Continued)**

Field	Description
Next Header	8-bit selector that identifies the type of header immediately following the IPv6 header. The Next Header uses the same values as the IPv4 protocol field for some protocols; for example, the values for TCP and UDP are the same for both IPv4 and IPv6. The Next Header values differ from IPv4 when IPv6 extension headers are identified or when IPv6 unique protocols, such as ICMPv6, are identified.
Hop Limit	8-bit unsigned integer that is decremented by 1 by each node that forwards the packet. If the hop limit is decremented to 0, the packet is discarded and the node sends the ICMPv6 message “Hop Limit Exceeded in transit” back to the sender.
Source Address	128-bit address of the originator of the packet
Destination Address	128-bit address of the intended recipient of the packet

Note: Type 0 IPv6 routing headers have been deprecated on the 7705 SAR (per RFC 5095).

3.1.3.3 Neighbor Discovery

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

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

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

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

Neighbor discovery is implemented within ICMPv6.

3.1.4 Router ID

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

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

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

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

- define the value using the **config>router>router-id** *ip-address* command
- define the system interface using the **config>router>interface** *ip-int-name* command (used if the router ID is not specified with the **config>router>router-id** *ip-address* command), or, if the 7705 SAR is acting as a DHCP client, allow the system interface to be defined dynamically by configuring the DHCP server-facing interface as unnumbered.

  A system interface (also referred to as the loopback address) must have an IP address with a 32-bit subnet mask. The system interface is assigned during the primary router configuration process when the interface is created in the logical IP interface context.
- if you do not specify a router ID, the last 4 bytes of the MAC address are used
- the router ID can be derived on the protocol level; for example, BGP

3.1.5 Autonomous Systems

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

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

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

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

Note: Within the router context, the 7705 SAR supports EBGP and IBGP. Within the VPRN context, the 7705 SAR supports EBGP but does not support IBGP. For information on configuring BGP within the router context, refer to the 7705 SAR Routing Protocols Guide, "BGP". For information on configuring BGP within the VPRN context, refer to the 7705 SAR Services Guide, "VPRN Services".

3.1.6 DHCP and DHCPv6

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

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

DHCPv6 is not based on, and does not use, the BOOTP protocol.

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

The 7705 SAR can act as a DHCP client, a DHCP or DHCPv6 Relay agent, or a local DHCP or DHCPv6 server.

When used as a CPE device, the 7705 SAR can act as a DHCP client to learn the IP address of the network interface. Dynamic IP address allocation is supported on both network and system interfaces.

OSPF, IS-IS, or RIP is used to advertise the system IP address over the network interface to the next-hop router. Static routing cannot be used because the network interface IP address is dynamic and can change during normal operation.

For DHCP, the DHCP protocol requires the client to transmit a request packet with a destination broadcast address of 255.255.255.255 that is processed by the DHCP server.

For DHCPv6, the DHCP protocol requires the client to transmit a request packet with a destination multicast address of ff02::1:2 (all DHCP servers and relay agents on the local network segment) that is processed by the DHCP server.

Since IP routers do not forward broadcast or multicast packets, this would suggest that the DHCP client and server must reside on the same network segment. However, for various reasons, it is sometimes impractical to have the server and client reside in the same IP network.

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

When the 7705 SAR is acting as a local DHCP server, it processes these DHCP broadcast or multicast packets and allocates IP addresses for the DHCP client as needed.

The 7705 SAR supports a maximum of 16 servers per node on the 7705 SAR-A, 7705 SAR-Ax, 7705 SAR-H, 7705 SAR-Hc, 7705 SAR-M, 7705 SAR-W, 7705 SAR-Wx, and 7705 SAR-X. The 7705 SAR supports a maximum of 62 servers per node on the 7705 SAR-8 Shelf V2 and on the 7705 SAR-18. Any Layer 3 interface configured using the global routing table or Layer 3 services supports up to 8 servers.

3.1.6.1 DHCP Relay and DHCPv6 Relay

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

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

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

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

3.1.6.1.1 DHCP Relay Agent Options

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

The 7705 SAR supports Option 60 and Option 61 as specified in RFC 2132. Option 60 is the vendor class identifier, which can contain information such as the client’s hardware configuration. Option 61 is the client identifier.

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

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

3.1.6.2 Local DHCP and DHCPv6 Server

The 7705 SAR supports local DHCP server functionality on the base router and on access IP interfaces associated with VPRN, by dynamically assigning IPv4 or IPv6 addresses to access devices that request them. This standards-based, full DHCP server implementation allows a service provider the option to decentralize IP address management into the network. The 7705 SAR can support public and private addressing in the same router, including overlapped private addressing in the form of VPRNs in the same router.

The 7705 SAR acts as a DHCP server or a DHCPv6 server.

An administrator creates pools of addresses that are available for assigned hosts. Locally attached hosts can obtain an address directly from the server. Routed hosts receive addresses through a relay point in the customer's network.

When a DHCP server receives a DHCP message from a DHCP Relay agent, the server looks for a subnet to use for assigning an IP address. If configured with the **use-pool-from-client** command, the server searches Option 82 information for a pool name. If a pool name is found, an available address from any subnet of the pool is offered to the client. If configured with the **use-gi-address** command, the server uses the gateway IP address (GIADDR) supplied by the Relay agent to find a matching subnet. If a subnet is found, an address from the subnet is offered to the client. If no pool or subnet is found, then no IP address is offered to the client.

When a DHCPv6 server receives a DHCP message from a DHCPv6 Relay agent, the server looks for a subnet to use for assigning an IP address. If configured with the **use-pool-from-client** command, the server searches Option 17 information for a pool name. If a pool name is found, an available address from any subnet of the pool is offered to the client. If configured with the **use-link-address** command, the server uses the address supplied by the Relay agent to find a matching subnet prefix. If a prefix is found, an address from the subnet is offered to the client. If no pool or prefix is found, then no IP address is offered to the client.

IPv4 and IPv6 address assignments are temporary and expire when the configured lease time is up. The server can reassign addresses after the lease expires.

If both the **no use-pool-from-client** command and the **no use-gi-address** command or **no use-link-address** command are specified, the server does not act.

3.1.6.2.1 DHCP and DHCPv6 Server Options

Options and identification strings can be configured on several levels.

DHCP servers support the following options, as defined in RFC 2132:

- Option 1—Subnet Mask
- Option 3—Default Routers
- Option 6—DNS Name Servers
- Option 12—Host Name
- Option 15—Domain Name
- Option 44—Netbios Name Server
- Option 46—Netbios Node Type Option
- Option 50—IP Address
- Option 51—IP Address Lease Time
- Option 53—DHCP Message Type
- Option 54—DHCP Server IP Address
- Option 55—Parameter Request List
- Option 58—Renew (T1) Timer
- Option 59—Renew (T2) Timer
- Option 60—Class Identifier
- Option 61—Client Identifier

DHCP servers also support Suboption 13 Relay Agent Information Option 82 as specified in RFC 3046, to enable the use of a pool indicated by the DHCP client.

DHCPv6 servers support the following options, as defined in RFC 3315:

- Option 1—OPTION_CLIENTID
- Option 2—OPTION_SERVERID
- Option 3—OPTION_IA_NA
- Option 4—OPTION_IA_TA
- Option 5—OPTION_IAADDR

- Option 6—OPTION_ORO
- Option 7—OPTION_PREFERENCE
- Option 8—OPTION_ELAPSED_TIME
- Option 9—OPTION_RELAY_MSG
- Option 11—OPTION_AUTH
- Option 12—OPTION_UNICAST
- Option 13—OPTION_STATUS_CODE
- Option 14—OPTION_RAPID_COMMIT
- Option 15—OPTION_USER_CLASS
- Option 16—OPTION_VENDOR_CLASS
- Option 17—OPTION_VENDOR_OPTS
- Option 18—OPTION_INTERFACE_ID
- Option 19—OPTION_RECONF_MSG
- Option 20—OPTION_RECONF_ACCEPT

These options are copied into the DHCP reply message, but if the same option is defined several times, the following order of priority is used:

1. subnet options
2. pool options
3. options from the DHCP client request

A local DHCP server must be bound to a specified interface by referencing the server from that interface. The DHCP server will then be addressable by the IP address of that interface. A normal interface or a loopback interface can be used.

A DHCP client is defined by the MAC address and the circuit identifier. This implies that for a certain combination of MAC and circuit identifier, only one IP address can be returned; if more than one request is made, the same address will be returned.

3.1.7 ICMP and ICMPv6

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

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

The 7705 SAR supports the ICMP capabilities described in Table 3.

Table 3 **ICMP Capabilities for IPv4**

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

The 7705 SAR supports the ICMPv6 capabilities described in Table 4.

Table 4 **ICMPv6 Capabilities for IPv6**

ICMPv6 Message	Description
Destination unreachable	Generated by a router to inform the source host that the destination is unreachable for a specified reason, other than congestion
Packet too big	Generated by a router in response to a packet that it cannot forward because the packet is larger than the MTU of the outgoing link.
Time exceeded	Generated by a router to inform the source of a packet that was discarded because the hop limit was exceeded in transit

Table 4 **ICMPv6 Capabilities for IPv6 (Continued)**

ICMPv6 Message	Description
Parameter problem	Generated by a router to inform the source of a packet that the packet was discarded due to a problem with a field in the IPv6 header or extension header that prevented it from processing the packet
Echo request/Echo reply	Used by the ping utility to test whether a host is reachable across an IP network and to measure the round-trip time for packets sent from the local host to a destination node
Neighbor Discovery ICMPv6 Messages	
Router solicitation	Sent by a host, when an interface is enabled, to request routers to generate router advertisements immediately rather than at their next scheduled time
Router advertisement	Sent by a router to advertise its presence as well as link and Internet parameters, periodically or in response to a router solicitation message
Neighbor solicitation	Sent by a node to determine the link-layer address of a neighbor or to verify that a neighbor is still reachable
Neighbor advertisement	Sent by a node in response to a neighbor solicitation message Nodes can also send unsolicited neighbor advertisements to announce a link-layer address change

3.1.8 Static Routes, Dynamic Routes, and ECMP

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

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

Equal-Cost Multipath Protocol (ECMP) refers to the distribution of packets over two or more egress links that share the same routing cost. ECMP is supported on static routes and dynamic (OSPF, IS-IS, and BGP) routes. The 7705 SAR supports ECMP for both LDP and IP traffic.

ECMP for LDP can be used to distribute MPLS traffic across the links in order to balance the traffic load. ECMP for LDP load-balances traffic across all equal-cost links based on the output of the hashing algorithm using the allowed inputs, based on the service type. For detailed information, refer to the 7705 SAR Interface Configuration Guide, “LAG and ECMP Hashing”. Refer also to the 7705 SAR MPLS Guide, “ECMP Support for LDP”, for more information.

For IP-routed traffic, as shown in Table 15 in the 7705 SAR Interface Configuration Guide, “LAG and ECMP Hashing”, the 7705 SAR load-balances the traffic over multiple equal-cost links with a hashing algorithm that uses header fields from incoming packets to calculate which link to use. By adding additional fields to the algorithm, the randomness of the results can be increased to ensure a more even distribution of packets across available links. ECMP for IP allows load balancing to be configured across all IP interfaces at the system level or interface level on the network side. Configuration at the interface level overrides the system-level settings for the specific interface. IP ECMP is supported on all 7705 SAR adapter cards and platforms.

Note: For VPLS and VLLs, and for Layer 3 spoke-SDP termination in IES and VPRN services, hashing is done on the service ID.

Interfaces on the system can have any mixture of load-balancing configurations, including having load balancing disabled. Router updates often cause interface load-balancing configuration changes. The 7705 SAR will automatically continue processing packets using the new interface configuration.

ECMP is configured on the interface but is agnostic to the underlying SAP, spoke SDP, or VPLS binding. ECMP configuration is maintained even if the binding type changes.

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

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

3.1.8.1 Static Route Resolution Using Tunnels

Static route packets can be forwarded to an indirect next hop over a tunnel programmed in the TTM using the **config>router>static-route-entry>tunnel-next-hop** command.

If the **tunnel-next-hop** context is enabled and the **resolution** command under this context is set to **any**, any supported tunnel type in the static route context can be selected following the TTM preference. If **resolution** is set to **disabled**, the tunnel binding is removed and resolution to the next hop resumes in the RTM. If **resolution** is set to **filter**, the route can be bound to a subset of active tunnels in the TTM, determined by the **resolution-filter** configuration in the **tunnel-next-hop** context.

The following tunnel types are supported in the static route context: LDP, RSVP-TE, SR-ISIS, SR-OSPF, and SR-TE.

See Router Global Commands for more information on the **tunnel-next-hop** command.

3.1.8.2 Enabling ECMP

The ECMP decision is performed at the ingress point on the node; therefore, ECMP must always be enabled on the ingress interface.

To enable LDP and GRT IP ECMP, the **config>router>ecmp** command is used.

To enable IP ECMP on a per-IP, next-hop basis (far-end PE) under the IP-VPRN context, the **config>service>vprn>ecmp** command is used.

For LDP ECMP, the **lsr-load-balancing** command under the system context enables optional LSR load balancing for the node. The **lsr-load-balancing** command under the router interface context overrides the system configuration for the specified interface.

For IP ECMP, the **l4-load-balancing** command under the system context enables optional Layer 4 load balancing for the node. The **l4-load-balancing** command under the router interface context, IES service interface context, or VPRN service interface context overrides the system configuration for the specified interface.

For IP ECMP, the **teid-load-balancing** command can be configured under the router interface context, IES interface context, and VPRN interface context.

For both LDP and IP ECMP, the **system-ip-load-balancing** command can be configured under the system context.

For information on the load-balancing commands, see Router Interface Commands, the 7705 SAR Basic System Configuration Guide, “System Information and General Commands”, and the 7705 SAR Services Guide, “VLL Services Command Reference”, “VPLS Command Reference”, “IES Command Reference”, and “VPRN Services Command Reference”.

3.1.9 IGP-LDP and Static Route-LDP Synchronization

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

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

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

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

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

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

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

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

3.1.10 Bidirectional Forwarding Detection (BFD)

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

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

If the configured number of consecutive BFD missed messages is reached, the route to the peer is declared not active. For centralized and line card BFD sessions, failure detection is propagated to all impacted upper layer protocols within a few milliseconds. Upper layer protocols act on failure information as soon as it is made available by BFD.

The v-port on the 2-port 10GigE (Ethernet) Adapter card and on the 2-port 10GigE (Ethernet) module is linked to the ring ports through the add/drop port, therefore its operational status—always operationally up—is not dependent on the status of the ring ports. Hence a ring port failure will not necessarily trigger an action at the v-port.

To ensure that there is fast detection of any Layer 2 failure and that protocols on the v-port will react to the failure, you must run health-check tests or OAM tests with the peer or peers at the far end. For example, BFD must be configured between the v-port and the far-end IP interface. The use of health-check tests to the far-end interface will trigger upper layer protection mechanisms on the v-port, where the behavior will be comparable to an intermediate Layer 2 transport network failure on any other Ethernet port.

For IPv4, BFD is supported on static routes, OSPF, IS-IS, BGP, PIM, RSVP-TE, L-LDP, and T-LDP. For IPv6, BFD is supported on static routes, IPv6 interfaces, L-LDP, T-LDP, and OSPFv3. The 7705 SAR also supports centralized BFD on Layer 3 spoke SDP interfaces. This capability allows BFD on Layer 3 spoke SDP interfaces to ride over the applicable tunnel and the configured spoke SDP to the far-end node where the spoke SDP is terminated. It offers a fast way to detect failures on Layer 3 interfaces riding over spoke SDPs; for example, service traffic running over an LSP tunnel.

Note:

- For network topologies where the BGP and/or T-LDP peer IP address is not a direct next hop (that is, the peer IP address is not an interface IP address but is either a system IP address or loopback IP address, or is multiple hops away), BFD automatically uses a centralized session to keep track of far-end IP address availability.
- Centralized next-hop BFD for static forwarding entries, or for OSPF or IS-IS routing protocols, is not supported on any loopback or system interface regardless of the configured mode (access or network) when the loopback interfaces have no physical associated ports. However, multi-hop centralized BFD sessions (for example, BGP, T-LDP) can make use of any loopback interface.

3.1.11 Seamless BFD

The 7705 SAR supports seamless BFD (S-BFD) as defined in RFC 7880. S-BFD is a form of BFD that avoids the negotiation and state establishment that is required for BFD sessions. The BFD session discriminator is predetermined and other mechanisms are used to distribute the discriminators to a remote network entity. This allows client applications or protocols to more quickly initiate and perform connectivity tests. Furthermore, a per-session state is maintained only at the head end of an S-BFD session. The tail end simply reflects BFD control packets back to the head end.

An S-BFD session is established between an initiator and a reflector. To participate in an S-BFD session, a mapping table of remote discriminators to far-end peer IP addresses must be statically configured on the 7705 SAR. The S-BFD initiator can begin sending BFD packets when it knows the reflector discriminator at the far-end node.

The 7705 SAR can be configured to act as a reflector. Only one reflector instance is supported per router and a discriminator is assigned to the reflector. Each of the initiators on the router is also assigned a discriminator.

Seamless BFD sessions are created at the request of a client application such as MPLS. This section describes the base S-BFD configuration that is required on initiator and reflector routers in order to participate in an S-BFD session. Application-specific configuration is required to create S-BFD sessions; for information, refer to the 7705 SAR MPLS Guide, “Seamless BFD for SR-TE LSPs”.

3.1.11.1 S-BFD Reflector Configuration and Behavior

The S-BFD reflector is configured using the following CLI commands:

```
configure
   bfd
      seamless-bfd
        [no] reflector <name>
                  description <string>
                  discriminator <value>
                  local-state {up | admin-down}
                  [no] shutdown
```

S-BFD reflection is enabled on the router when the S-BFD discriminator is configured. The discriminator value is configured from a defined range.

Note: Only one reflector discriminator is supported per router. The reflector cannot be administratively enabled with the **no shutdown** command until the discriminator is configured.

When the router receives an S-BFD packet from the initiator and the value in the YourDiscriminator field in the packet matches the configured **discriminator** value on the local router, the local router will send the S-BFD packet back to the initiator via a routed path. The State field in the reflected packet is populated with either the Up or AdminDown value based on the **local-state** configuration.

When the S-BFD reflector returns the S-BFD packet to the initiator, the source and destination UDP ports are swapped in the S-BFD response; that is, the received source port becomes the transmitted destination port and the received destination port becomes the transmitted source port.

S-BFD control packets are discarded when the reflector is not configured, or is shut down, or when the YourDiscriminator field does not match the discriminator of the reflector. Both IPv4 and IPv6 addresses are supported, but for IPv6, the reflector can only reflect BFD control packets with a global unicast destination address (link-local addresses are not supported).

3.1.11.2 S-BFD Initiator Global Configuration

Before an application can request the establishment of an S-BFD session, a mapping table of remote discriminators to far-end peer IP addresses must exist on the router. This is statically configured using the following CLI commands:

```
configure>router>bfd
   seamless-bfd
      peer <ip-address> discriminator <remote-discriminator>
      peer <ip-address> discriminator <remote-discriminator>
      ...
      exit
```

With S-BFD, no session setup is required. The S-BFD initiator immediately begins sending S-BFD packets when it knows the far-end reflector discriminator. The initiator state goes from AdminDown to Up when it begins to send S-BFD packets.

The S-BFD initiator sends S-BFD packets to the reflector using the following fields:

- Src IP — the local session IP address; for IPv6, this is a global unicast address belonging to the node
- Dst IP — the configured reflector IP address
- MyDiscriminator — the locally assigned discriminator value
- YourDiscriminator — the configured reflector discriminator value

When the initiator receives a valid response from the reflector with an Up state, the initiator declares the S-BFD session up. When the initiator receives a valid response from the reflector with an AdminDown state, the initiator declares the S-BFD session down and reduces the transmission interval but does not consider the session failed.

If the initiator fails to receive a certain number of responses as determined by the BFD multiplier in the BFD template for the session, the initiator declares the S-BFD session failed.

If any of the discriminators change, the session is taken down and the router attempts start a new session with the new values.

If the reflector discriminator is changed at the far-end peer, the session fails. If the reflector discriminator is changed at the far-end peer and the mapping has not been updated locally before the system checks for a new reflector discriminator from the local mapping table, the session is bounced and brought up with the new values.

If any of the discriminators are deleted, the corresponding S-BFD sessions are deleted.

3.1.11.3 S-BFD Session Configuration

An application that requires an S-BFD session must provide sufficient information to BFD so that it can create a unique S-BFD session to a remote IP address associated with the application object, such as an LSP. The session type (S-BFD) is determined by the application. BFD checks that the BFD template parameters are appropriate for the requested session type.

An S-BFD session is configured using the following parameters in the **config>router>bfd>bfd-template** context:

- multiplier
- receive interval
- transmission interval
- type

An S-BFD session must also include the following parameters configured in the **config>router>bfd>seamless-bfd** context:

- remote reflector IP address
- remote reflector discriminator

3.1.12 IP Fast Reroute (FRR)

IP Fast Reroute (FRR) protects against link or node failures in an IP network by precalculating a backup route to use when the primary next hop is not available. Both routes are populated in the RTM.

Without FRR, when a link or node failure occurs in a routed network, there is a period of disruption to the delivery of traffic until the network reconverges. Packets may be dropped or looped during this time, which can last hundreds of milliseconds.

IP FRR uses a Loop-Free Alternate (LFA) backup next hop to forward in-transit IP packets as soon as the primary next-hop failure is detected and the backup is invoked. This means that a node resumes forwarding IP packets to a destination prefix without waiting for the routing convergence. Convergence times should be similar to RSVP-TE FRR, in the tens of milliseconds.

When any of the following occurs, the backup LFA is enabled:

- an OSPF or IS-IS interface goes operationally down, due to either a physical failure or a local administrative shutdown
- a BFD session to a next hop times out when BFD is enabled on the interface

Refer to RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*, for more information on LFAs.

IP FRR is supported on IPv4 and IPv6 OSPF and IS-IS prefixes and on VPN-IPv4 OSPF prefixes forwarded in the base router instance. IP FRR also provides an LFA backup next hop for the destination prefix of a GRE tunnel used in an SDP or in VPRN auto-bind.

3.1.12.1 ECMP vs FRR

If ECMP is enabled, which provides multiple primary next hops for a prefix, IP FRR is not used. That is, the LFA next hops are not populated in the RTM and the ECMP paths are used instead.

3.1.12.2 IGP Shortcuts (RSVP-TE Tunnels)

IGP shortcuts are an MPLS functionality where LSPs are treated like physical links within IGPs; that is, LSPs can be used for next-hop reachability. If an RSVP-TE LSP is used as a shortcut by OSPF or IS-IS, it is included in the SPF calculation as a point-to-point link for both primary and LFA next hops. It can also be advertised to neighbors so that the neighboring nodes can also use the links to reach a destination via the advertised next hop.

IGP shortcuts can be used to simplify remote LFA support and simplify the number of LSPs required in a ring topology.

When both IGP shortcuts and LFA are enabled under OSPF or IS-IS, and IP FRR is also enabled, the following applies:

- a prefix that is resolved to a direct primary next hop can be backed up by a tunneled LFA next hop
- a prefix that is resolved to a tunneled primary next hop will not have an LFA next hop; it relies on RSVP-TE FRR for protection

3.1.12.3 IP FRR Configuration

To configure IP FRR, LFA calculation by the SPF algorithm must first be enabled under the OSPF, OSPFv3, or IS-IS protocol level with the command:

config>router>ospf>loopfree-alternate
or
config>router>ospf3>loopfree-alternate
or
config>router>isis>loopfree-alternate

LFA can also be enabled on an OSPF or OSPFv3 instance within a VPRN service with the command:

config>service>vprn>ospf>loopfree-alternate
or
config>service>vprn>ospf3>loopfree-alternate

Next, IP FRR must be enabled to use the LFA next hop with the command **config>router>ip-fast-reroute**.

If IGP shortcuts are used, they must be enabled under the OSPF or IS-IS routing protocol. As well, they must be enabled under the MPLS LSP context, using the command **config>router>mpls>lsp>igp-shortcut**.

For information on LFA and IGP shortcut support for OSPF and IS-IS, refer to the 7705 SAR Routing Protocols Guide, “LDP and IP Fast Reroute for OSPF Prefixes” and “LDP and IP Fast Reroute for IS-IS Prefixes”.

The 7705 SAR supports both IP FRR and LDP FRR; for information on LDP FRR, refer to the 7705 SAR MPLS Guide, “LDP Fast Reroute (FRR)”.

3.2 Configuring Security Parameters

The 7705 SAR supports a number of mechanisms for node security, including Access Control Lists (ACLs), Network Address Translation (NAT), and stateful, zone-based firewalls. For information about ACLs, see Configuring Filter Policies. For more details about NAT, see NAT Security.

Firewalls extend ACL filtering by ensuring that pass-through IP traffic between an inside (trusted private) network and an outside (untrusted public) network does not pose a security risk.

NAT and firewall security configurations are both based on zones. Zones segment a network, making it easier to control and organize traffic. A zone consists of a group of Layer 2 endpoints or Layer 3 interfaces with common criteria, bundled together. Security policies, which define a set of rules that determine how NAT or firewall should direct traffic, can be applied to the entire zone or to multiple zones. Layer 3 zones support both NAT and firewall security policies. Layer 2 zones support only firewalls. To enable NAT or firewall functionality, security policy and profile parameters must be configured under the **config>security** context in the CLI, and a security zone must be configured under one or more of the following contexts:

- **config>router>zone**
- **config>service>epipe>zone**
- **config>service>vpls>zone**
- **config>service>vprn>zone**
- **config>service>ies>zone**

Layer 2 and Layer 3 firewalls share system resources; that is, they share the maximum number of policies, profiles, and session ID space supported by the system.

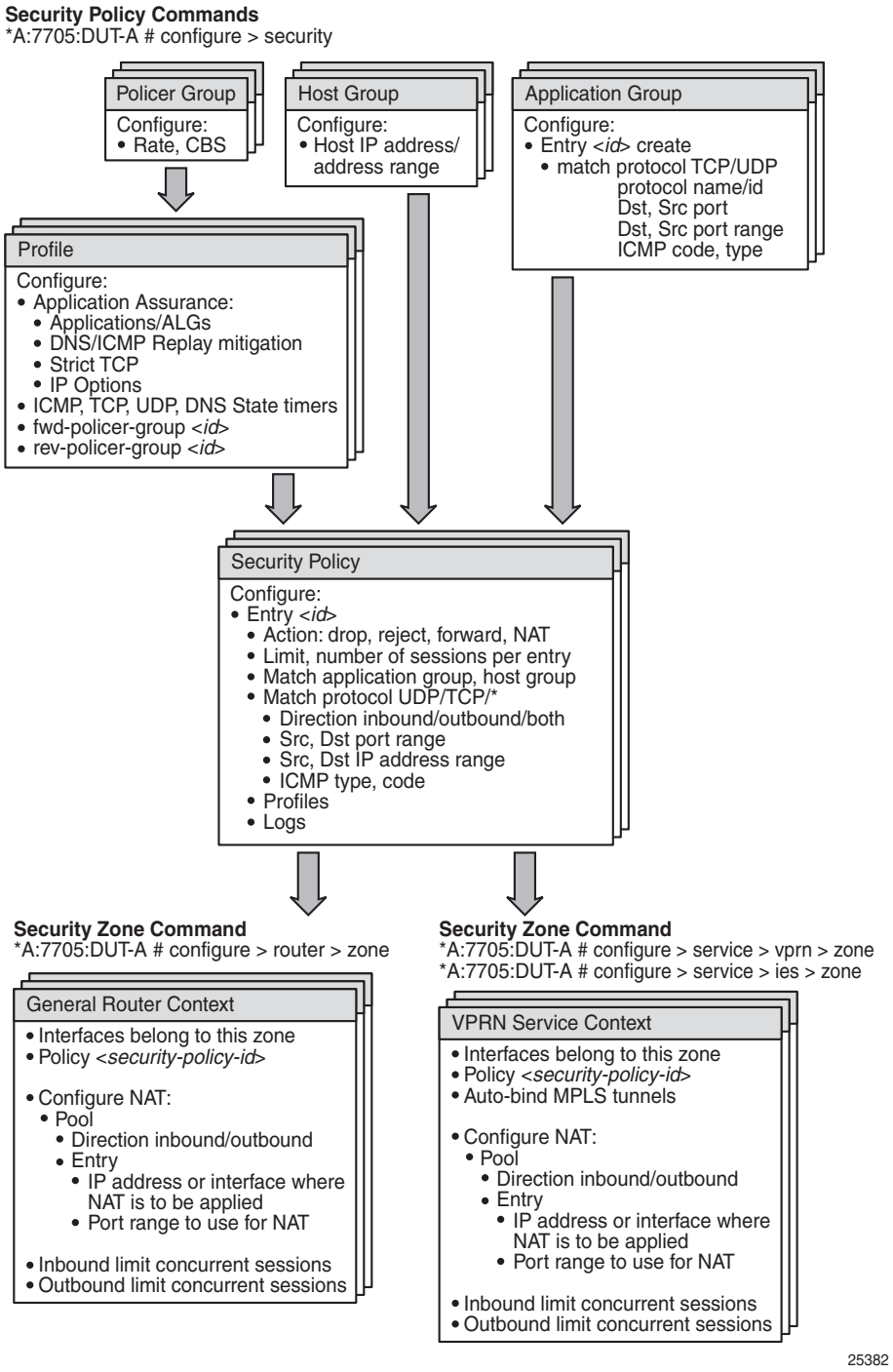
Figure 2 shows the relationship between the configurable elements for firewall and NAT security.

This section describes the following topics:

- Hardware Support
- Security Zone Configuration
- Security Session Creation
- Application Groups
- Host Groups
- Security Policy Policing

- Security Profiles
- Security Policies
- Bypass Policies for a Firewall in a Layer 2 Service
- Security Session Resource Alarms
- Security Logging
- Firewall Debugging
- NAT Security
- Multi-Chassis Firewall

Figure 2 **Firewall and NAT Security Configuration for the 7705 SAR**



3.2.1 Hardware Support

NAT and firewall security functionality is supported on the following cards and platforms:

- on the 7705 SAR-8 Shelf V2 and the 7705 SAR-18:
  - 2-port 10GigE (Ethernet) Adapter card
  - 6-port Ethernet 10Gbps Adapter card
  - 8-port Gigabit Ethernet Adapter card, version 3
  - 10-port 1GigE/1-port 10GigE X-Adapter card, version 2 (7705 SAR-18 only)
  - Packet Microwave Adapter card
- 7705 SAR-Ax
- 7705 SAR-H
- 7705 SAR-Hc
- 7705 SAR-Wx
- 7705 SAR-X

3.2.2 Security Zone Configuration

NAT and firewall security configuration is based on zones. Zones segment a network, making it easier to control and organize traffic. A zone consists of a group of Layer 2 endpoints or Layer 3 interfaces with common criteria, bundled together. Security policies, which define a set of rules that determine how NAT or a firewall should direct traffic, can be applied to the entire zone or multiple zones.

A zone is created by adding at least one Layer 2 endpoint or Layer 3 interface to the zone configuration. Multiple zones can be created within each Layer 3 service or within the router context. Layer 2 services support only one zone. Layer 2 endpoints or Layer 3 interfaces from different services cannot be grouped into a single common zone. Table 5 lists the supported interfaces and endpoints that can be added to zones in each CLI context for NAT or firewall.

Table 5 **Security Zone Interfaces and Endpoints per Context**

CLI Context	Interface/Endpoint Type	NAT	Firewall
Router	Layer 3	✓	✓

Table 5 **Security Zone Interfaces and Endpoints per Context (Continued)**

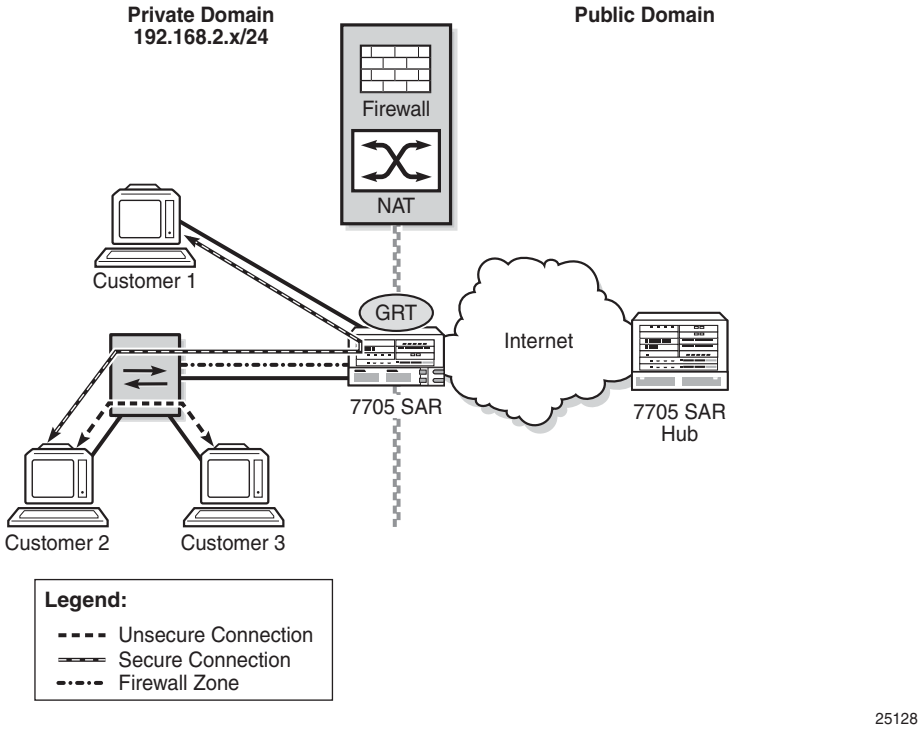
CLI Context	Interface/Endpoint Type	NAT	Firewall
Epipe	SAP		✓
	Spoke-SDP termination		✓
VPLS	SAP		✓
	Spoke-SDP termination		✓
	Mesh SDP		✓
	EVPN		
VPRN	SAP	✓	✓
	Spoke-SDP termination	✓	✓
	IPSec private	✓	✓
	IPSec public	✓	
	Routed VPLS	✓	✓
IES	SAP	✓	✓
	Spoke-SDP termination	✓	✓
	IPSec public	✓	
	Routed VPLS	✓	✓

Note: A group of endpoints used for pseudowire redundancy cannot be added to a zone configured under an Epipe.

A zone configured within the router context is typically used to provide security functionality between an outside (insecure) network such as an ISP network or Layer 2/Layer 3 leased line network, and an inside (secure) network such as a corporate LAN or a small cell wireless network.

Figure 3 shows a 7705 SAR connected to an insecure network (the public Internet), via the GRT. A firewall configured on the 7705 SAR protects the private access network from any connection that is not part of the 7705 SAR security policy.

Figure 3 **Firewall Protection of a Private Access Network**

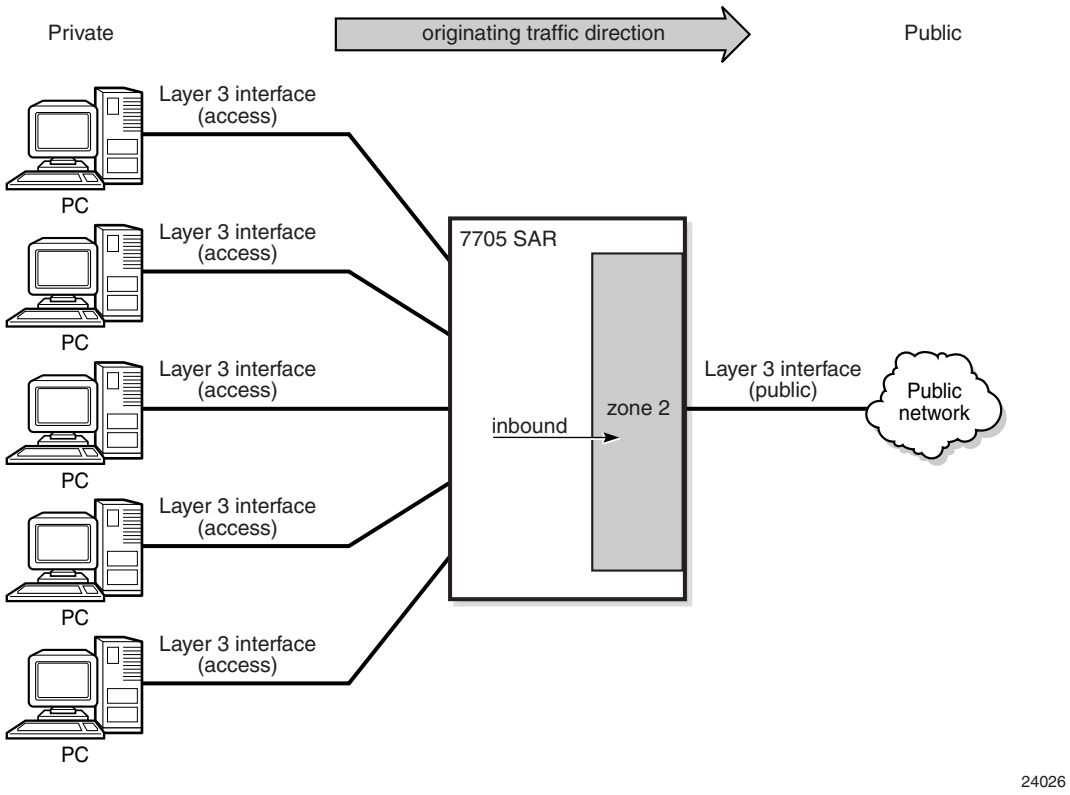


For information about creating a security zone for VPRN, IES, VPLS, or Epipe services, refer to the applicable service chapters in the 7705 SAR Services Guide.

Security policies can be configured based on traffic entering (inbound) the zone, leaving (outbound) the zone, or both inbound and outbound traffic. A zone can be configured so that all traffic inbound to the zone has NAT and/or firewall applied to it based on the security policy configured for that zone. A zone can also be configured so that all traffic leaving the zone has NAT and/or firewall applied to it. And, a zone can be configured so that all traffic both inbound and outbound has firewall applied to it.

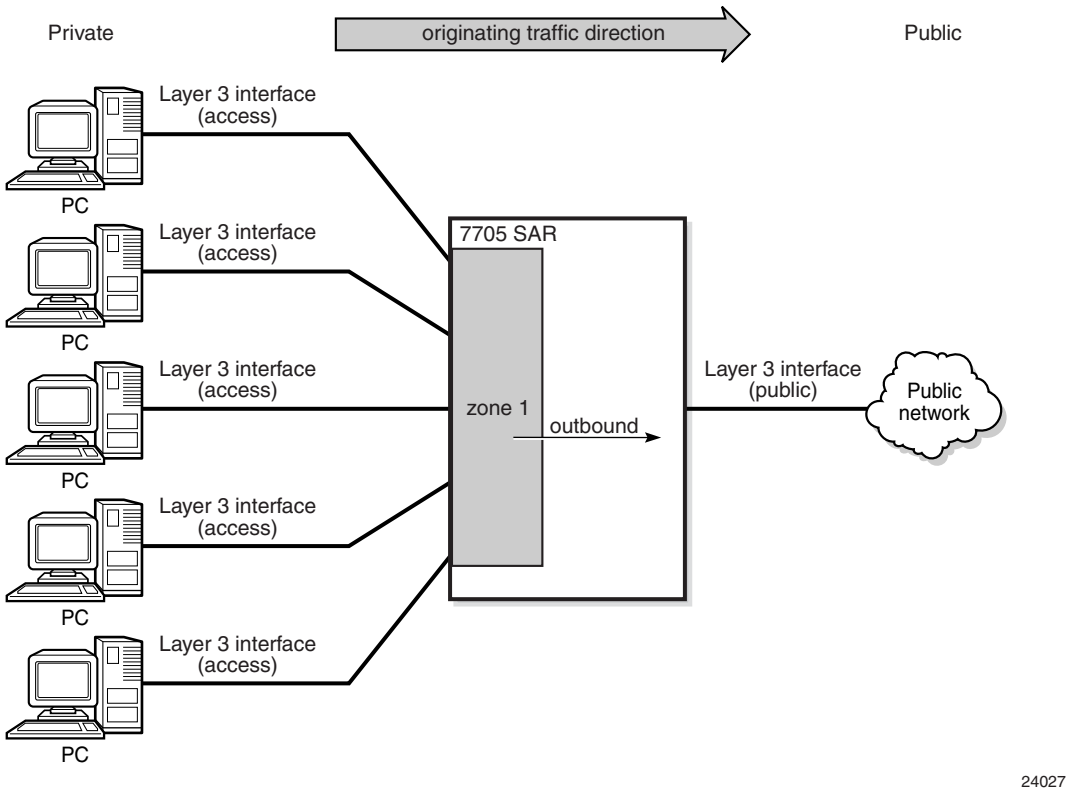
An example of inbound zone direction is shown in Figure 4. All traffic entering zone 2 has NAT applied to it based on the configured NAT policy assigned to zone 2.

Figure 4 **Zone Direction (Inbound)**



An example of outbound zone direction is shown in Figure 5. All traffic leaving zone 1 has NAT applied to it based on the configured NAT policy assigned to zone 1.

Figure 5 **Zone Direction (Outbound)**



3.2.3 Security Session Creation

A firewall or NAT security session is established by extracting packets to the CSM and matching them against the rules configured in a security policy. Packet extraction is based on zone configuration. If a packet is inbound to or outbound from a security zone, the packet will be extracted to the CSM and examined by the firewall/NAT engine on the CSM.

If the extracted packet matches the criteria defined in the security policy, a connection session is set up using lookup criteria that are specific to the packet type and an accompanying action. For example, an IP packet uses a 6-tuple lookup of source IP address, destination IP address, source port, destination port, protocol, and VRF (where VRF 0 is the base routing table).

Depending on the match criteria and action, a copy of the session is downloaded to the datapath. For example, a session is not downloaded to the datapath if the action in the security policy is configured as **reject**. When the session is downloaded to the datapath, there is no further extraction to the CSM for examination; any subsequent packet matching the 6-tuple of the session occurs on the datapath session.

Some connection sessions are set up using more criteria in the lookup than 6-tuple while other sessions are set up using a 4-tuple lookup. Table 6 lists the session type and session tuple signature.

Table 6 **Security Session Type and Session Tuple Signature**

Session Type	Session Tuple Signature
IP	VRF, source IP address, destination IP address, and protocol
UDP/TCP/SCTP	VRF, source IP address, destination IP address, source port, destination port, and protocol
ICMP	VRF, source IP address, destination IP address, and ICMP request ID
DNS	VRF, source IP address, destination IP address, source port, destination port, protocol, and DNS transaction ID

Some connection sessions require CSM extraction of every packet; for example, a connection that requires strict TCP. For this type of CSM connection, the TCP session state and sequence number must be examined for every packet on that connection. The connection session is downloaded to the datapath and marked for extra processing. The datapath then extracts every packet on this session to the firewall engine on the CSM. The throughput rate of these CSM firewall sessions is lower than that of datapath firewall sessions. Datapath sessions can process traffic at approximately the line rate. Any connection session that uses strict TCP is not hot-redundant and will time out after an activity switch.

Both CSM and datapath sessions are stateful as they can both read into TCP/UDP states and close the session based on the timers configured for that session.

On the 7705 SAR-8 Shelf V2 and 7705 SAR-18, security sessions survive a CSM redundancy switch; however, security sessions configured with strict TCP do not.

Zones can be configured to have session limits on a per-direction basis, in order to limit potential attacks.

3.2.3.1 Directionally Aware Security Behavior

A security session can be directionally aware. For example, a firewall security policy entry can be configured to allow packets with source IP address X and source port Y that are traveling from the private network to the public network to traverse the firewall. This means that any traffic arriving from the outside network on IP address X and port Y is denied entry to the inside network. However, a host in the private network can create a session from inside to outside for IP address X and port Y. Once this inside-to-outside session is created, traffic with IP address X and port Y traveling in the reverse direction (from outside to inside) is now allowed.

Similarly with NAT, a source NAT policy entry can be created to apply NAT on all arriving packets with source IP address X and source port Y to an outside source IP address A and source port B. When the first packet with IP address X and port Y arrives, NAT creates an inside-to-outside session and punches a hole through the firewall for that specific IP address and port number, thus allowing all packets to be transmitted from the inside network to the outside network.

3.2.3.2 TCP MSS Configuration and Adjustment

Typically, the MTU in a private LAN is larger than the MTU of a public network; the MTU of a private LAN is usually 1500 bytes whereas the MTU of a public network is usually less than 1500 bytes. In addition, packets destined for the public network may have an additional header, such as a transport tunnel, appended to the original packet. These two factors can cause the TCP/IP packet to become fragmented when entering the public network. Fragmentation is not desirable for TCP applications where the server needs a lot of processing power to reassemble the fragmented packets.

To avoid fragmentation, the maximum segment size (MSS) of application data in a TCP connection can be adjusted. Applications use the MSS to calculate the maximum number of data bytes (not including the header) that can be transmitted in a single packet. By lowering the MSS value, an outgoing packet's MTU can be made smaller than the public network MTU, ensuring that the packets entering the public network will not be fragmented.

The 7705 SAR supports TCP MSS adjustment. When acting as a CE router, the 7705 SAR can insert or modify the MSS value in the header of a TCP SYN or SYN-ACK packet. The sending and receiving CE routers set their MSS based on the outgoing interface MTU. The routers exchange TCP SYN or SYN-ACK packets during TCP session negotiation, engaging in a three-way handshake to compare and then select the lowest MSS value.

On the 7705 SAR, MSS configuration and adjustment is supported on the following cards and platforms:

- on the 7705 SAR-8 Shelf V2 and the 7705 SAR-18:
  - 2-port 10GigE (Ethernet) Adapter card
  - 6-port Ethernet 10Gbps Adapter card
  - 8-port Gigabit Ethernet Adapter card, version 3
  - 10-port 1GigE/1-port 10GigE X-Adapter card, version 2 (7705 SAR-18 only)
  - Packet Microwave Adapter card
- 7705 SAR-Ax
- 7705 SAR-H
- 7705 SAR-Hc
- 7705 SAR-W
- 7705 SAR-Wx
- 7705 SAR-X

When the **tcp-mss** command is configured, the 7705 SAR can adjust the MSS field in the TCP SYN packet or SYN-ACK packet. The 7705 SAR can also insert the MSS field in the TCP SYN packet and SYN-ACK packet if the field is not present.

The command is supported in the general router, VPRN service, and IES CLI contexts; Table 7 lists the supported interface types for each context. The **tcp-mss** command is supported for TCP packets arriving on or leaving from MP-BGP tunnels in a VPRN.

Table 7 **MSS Configuration Interfaces per Context**

CLI Context	Interface Type
Router	Layer 3
VPRN	SAP
	Spoke-SDP termination
	IPSec private
IES	SAP
	Spoke-SDP termination

When the **tcp-mss** command is configured on an interface, TCP packets with a SYN or SYN-ACK flag will have the MSS value is adjusted or inserted, as follows.

- If the TCP session has no defined MSS, the 7705 SAR inserts the field in the TCP packet.
- If the MSS value of the TCP session arriving from an access interface is greater than the MSS value configured on the 7705 SAR interface, the TCP session MSS is overwritten with the lower value.
- If the MSS value of the TCP session arriving from an access interface is less than the MSS value configured on the 7705 SAR interface, the TCP session MSS does not change.

The command can be configured on an ingress interface, an egress interface, or both. When configured on both interfaces, the smallest MSS value is used.

Fragmented packets are not monitored for TCP MSS adjustment.

TCP MSS configuration and adjustment is supported for both IPv4 and IPv6 interfaces. Because the **tcp-mss** value is configured separately for each interface, it is possible to configure and enforce a different MSS value for IPv4 and IPv6.

3.2.4 Application Groups

An application group is a grouping of common criteria, such as the TCP/UDP port or ICMP code/type, used for a specific application. An application group is assigned to a security policy and application group criteria are matched in the policy. For further security, an application group can be configured with security profile parameters such as timeouts, fragmentation rules, and application assurance rules. Configuring an application group simplifies the configuration and management of firewall policies. An application group can be configured on the NSP NFM-P and downloaded to all routers at a particular network layer (either access or core) that require the same matching criteria.

3.2.5 Host Groups

A host group is a grouping of host IP addresses that can be added to a security policy. Configuring a host group simplifies the configuration of a security policy. Typically, service providers have a preassigned set of IP addresses that are allowed in the network. By creating a host group, a range of IP addresses or a single source/destination IP address is configured once and assigned to every edge router. The host group is added to the security policy as matching criteria.

3.2.6 Security Policy Policing

A private network can be infiltrated when an open port through the firewall is scanned and a DoS attack is initiated. The attack can use large amounts of bandwidth, starving existing connections of bandwidth and preventing other connections traversing through the firewall from using any bandwidth. To address this, a policer group can be configured against a profile and assigned to an entry within a security policy. All connections set up against that particular entry on the same adapter card or port are subjected to a policer rate and CBS buffer size. If the aggregate for one or more sessions using the policer group is exceeded, packets received beyond the policed rate are dropped and a log event is issued.

3.2.7 Security Profiles

Security profiles define security characteristics on the router, such as timers for different states of a TCP/UDP connection, application assurance parameter definitions, and whether to allow fragmented packets in a network. Security profiles can vary from subscriber to subscriber and are assigned to security policies, which are then applied to zones at the time the zone is created.

Note: Security profile 1 is the default profile and cannot be modified. By default, this profile is assigned to any security policy that does not have a profile.

3.2.7.1 Profile Timers

Timers are used to time out a NAT or firewall session and drop it. The 7705 SAR supports configurable timers for different connections. Timers can be idle or strict. Idle timers are activated by the lack of traffic. Strict timers are used for protocol state changes and are not affected by the presence of traffic. The supported timers are described in Table 8.

Table 8 **Security Profile Timers**

Timer	Description	Timer Type	CLI Command
ICMP request	Specifies the timeout for an ICMP session Default timeout: 1 min Minimum timeout: 1 min Maximum timeout: 5 min	Strict	icmp-request

Table 8 **Security Profile Timers (Continued)**

Timer	Description	Timer Type	CLI Command
Idle timeout	Specifies the timeout for a security session for IP packets that are not ICMP, TCP, or UDP Default timeout: 600 s Minimum timeout: 1 s Maximum timeout: 10800 s	Idle	other-sessions
TCP established	Specifies the timeout for a TCP session in the established state Default timeout: 2 h, 4 min Minimum timeout: 1 min Maximum timeout: 24 h	Idle	tcp-established
TCP SYN	Specifies the timeout applied to a TCP session in the SYN state Default timeout: 15 s Minimum timeout: 6 s Maximum timeout: 24 h	Strict	tcp-syn
TCP time wait	Specifies the timeout applied to a TCP session in a time-wait state Default timeout: n/a Minimum timeout: n/a Maximum timeout: 4 min	Strict	tcp-time-wait
TCP transitory	Specifies the idle timeout applied to a TCP session in a transitory state Default timeout: 4 min Minimum timeout: 1 min Maximum timeout: 24 h	Strict	tcp-transitory
UDP	Specifies the UDP mapping timeout Default timeout: 5 min Minimum timeout: 1 min Maximum timeout: 24 h	Idle	udp
UDP DNS	Specifies the timeout applied to a UDP session with destination port 53 Default timeout: 15 s Minimum timeout: 15 s Maximum timeout: 24 h	Idle	udp-dns

Table 8 **Security Profile Timers (Continued)**

Timer	Description	Timer Type	CLI Command
UDP initial	Specifies the timeout applied to a UDP session in its initial state Default timeout: 15 s Minimum timeout: 10 s Maximum timeout: 5 min	Strict	udp-initial

3.2.7.2 Application Assurance Parameters

The following application assurance parameters can be defined in a security profile:

- DNS
- ICMP
- IP options
- strict TCP

3.2.7.2.1 DNS

Each DNS session request received on the 7705 SAR should have only a single response. When the **reply-only** command is configured in the **config>security>profile>aa>dns** CLI context, the firewall discards any additional responses, which can help prevent a DNS replay attack. The firewall will permit a single request and a single reply; any other DNS packets with the same DNS request ID that are received on that session will be dropped. See Table 6 for the match criteria for a DNS session.

3.2.7.2.2 ICMP

ICMP replay attacks can be prevented using two mechanisms:

- limiting the number of ICMP requests and the number of replies to ICMP requests with the **request-limit** command
- limiting the number of ICMP type 3 replies to ICMP or IP sessions with the **limit-type3** command

For each ICMP request received, the 7705 SAR creates an ICMP session based on the ICMP packet identifier field and source and destination IP addresses. The 7705 SAR restricts the number of packets for that session based on the limit configured in the **request-limit** command. Any request received beyond the configured limit for that session is blocked. For example, if the ICMP request limit is set to 2, only two ping requests and replies can be transmitted from that ICMP session, while the ICMP session has not timed out. This ensures that an external attacker cannot replay the ICMP reply packet repeatedly to the source of the ICMP request.

Note: It is recommended that the ICMP session timeout be set to equal the latency or delay of the network so that the session times out very quickly, and also that the timer type be set to strict so that the ICMP session times out strictly within the timer value.

The 7705 SAR can limit the number of ICMP type 3 replies for ICMP and IP sessions. For every packet arriving at the firewall, the 7705 SAR creates a 6-tuple session. For regular IP packets, these sessions are uniquely identified using the 6-tuple. For ICMP packets, these sessions are identified using the source IP address, the destination IP address, and the ICMP identifier field. If these packets are discarded after traversing the firewall (for example, because the destination is unreachable or fragmentation is not allowed), an ICMP type 3 packet is generated and sent back to the originator.

The ICMP type 3 packet usually has at least the first 8 octets of the original datagram in the payload of its packet. When the ICMP type 3 packet arrives at the 7705 SAR, the 7705 SAR examines the packet and its payload to find the original packet that triggered the error and tries to find the corresponding session for that packet. If it does, it counts the ICMP type 3 packet against the session. The 7705 SAR allows only 15 ICMP type 3 packets through for each original packet. If the 7705 SAR does not find the session corresponding to the packet that triggered the error, it discards the ICMP type 3 packet.

3.2.7.2.3 IP Options

Traffic on the 7705 SAR can be firewalled based on the IP options in the IP packet header. When IP option names or bit mask values are configured in a security profile using the **config>security>profile>aa>ip>options** command, only packets with the specified IP options are allowed through the firewall.

If the command is configured with the **permit-any** option (the default), the firewall does not examine the packet IP options and allows all packets through.

Table 9 lists the names and bit mask values of supported IP options. For more information, see the IANA website at: http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml

Table 9 **Supported IP Options**

IP Option Number	IP Option Value	IP Option Name	Bit Mask Value
0	0	EOOL – End of Options List	0x00000001
1	1	NOP – No Operation	0x00000002
2	130	SEC – Security	0x00000004
3	131	LSR – Loose Source Route	0x00000008
4	68	TS – Time Stamp	0x00000010
5	133	E-ESC – Extended Security	0x00000020
6	134	CIPSO – Commercial Security	0x00000040
7	7	RR – Record Route	0x00000080
8	136	SID – Stream ID	0x00000100
9	137	SSR – Strict Source Route	0x00000200
10	10	ZSU – Experimental Measurement	0x00000400
11	11	MTUP – MTU Probe	0x00000800
12	12	MTUR – MTU Reply	0x00001000
13	205	FINN – Experimental Flow Control	0x00002000
14	142	VISA – Experimental Access Control	0x00004000
15	15	Encode	0x00008000
16	144	IMITD – IMI Traffic Descriptor	0x00010000
17	145	EIP – Extended Internet Protocol	0x00020000

Table 9 **Supported IP Options (Continued)**

IP Option Number	IP Option Value	IP Option Name	Bit Mask Value
18	82	TR – Traceroute	0x00040000
19	147	ADDEXT – Address Extension	0x00080000
20	148	RTRALT – Router Alert	0x00100000
21	149	SDB – Selective Directed Broadcast	0x00200000
22	150	Unassigned	0x00400000
23	151	DPS – Dynamic Packet State	0x00800000
24	152	UMP – Upstream Multicast Packet	0x01000000
25	25	QS – Quick-Start	0x02000000
30	30	EXP – RFC3692-style experiment	0x40000000
30	94	EXP – RFC3692-style experiment	0x40000000
30	158	EXP – RFC3692-style experiment	0x40000000
30	222	EXP – RFC3692-style experiment	0x40000000

3.2.7.2.4 Strict TCP

A security profile on the 7705 SAR can be configured with strict TCP in order to monitor a TCP connection. With strict TCP configured, the 7705 SAR extracts all packets for that session to the CSM for further examination as defined by RFC 793. This parameter should be used under particular circumstances, such as a suspected DoS attack.

3.2.7.3 Application Level Gateway

When a 7705 SAR security profile is configured with Application Level Gateway (ALG), the firewall/NAT engine intercepts all upstream traffic destined for TCP port 21 (the FTP control channel), UDP port 69 (the TFTP port), or some other destination port configured to support ALG. All traffic matching the policy is extracted to the CSM for examination.

If the examined traffic is found to be an FTP control channel, the corresponding data channel is programmed to the datapath. When an FTP client sends the port command in the FTP control channel, the firewall/NAT ALG intercepts this command, creates a new mapping in the firewall/NAT table, and opens the data port based on the client port command. Firewalls configured in either passive or active mode must have ALG configured in order to allow the FTP datapath through the firewall. A temporary match rule for the FTP data port is placed on top of the security policy, and TCP timer configuration is inherited from ALG policy control timers. In short, the temporary data session inherits all the control session policy/profile configuration.

Trivial File Transfer Protocol (TFTP) is a simple File Transfer Protocol, which is implemented on top of the UDP/IP protocol and uses port 69. TFTP was designed to be small and easy to implement; therefore, it does not have most of the advanced features offered by more robust file transfer protocols such as FTP. TFTP requests from a client are always destined for UDP port 69 on the server. The server responds by sending an ACK and/or the data on a random port. The 7705 SAR firewall and the ALG are able to detect this random port and create a temporary rule to open the UDP port in the firewall.

The ALG security profile parameter can be configured as **auto**, **ftp**, or **tftp**.

When the parameter is configured as **auto** (the default), FTP or TFTP ALG is enabled on TCP port 21 (the default port for FTP) or UDP port 69 (the default port for TFTP). The firewall will enforce use of the ALG on the FTP or TFTP session for port translation, if NAT is being used, and for pin-hole operations.

When the parameter is configured as **ftp**, FTP ALG is enabled on any TCP port being used for FTP. For example, if a security session has been configured for a DNAT mapping where the destination port is not TCP port 21, configuring the ALG security parameter as **ftp** allows the FTP ALG to be enabled on TCP ports or TCP port ranges so that the session can be treated as FTP and so that the ALG can perform the correct translation and pin-hole functions as required by FTP.

When the parameter is configured as **tftp**, TFTP ALG is enabled on any UDP port being used for TFTP.

Unlike auto ALG, where only the default FTP and TFTP ports are inspected for a potential ALG session, FTP ALG and TFTP ALG inspect all packets that match their policy's matching criteria. It is recommended that a specific destination port or port range be matched so that entire port ranges are not left open for potential attackers.

The following example shows a recommended configuration for incoming (DNAT) and outgoing FTP control.

```
*A:7705:Dut-A> config>security# info
----------------------------------------------
    logging
    exit
    profile 10 create
        name "ALG-FTP"
         application
            alg ftp
        exit
        timeouts
         exit
    exit
    policy 1 create
        name "Inbound Policy"
        entry 1 create
            description "match Local non-default FTP"
            match local protocol tcp
                dst-port eq 1024
            exit
            limit
            exit
            action nat destination 10.100.0.2 port 21
            profile "ALG-FTP"
            logging to zone
        exit
        entry 2 create
            description "match forward FTP Ctl"
            match protocol tcp
                direction zone-inbound
                dst-port eq 1024
            exit
            limit
            exit
            action forward
            profile "ALG-FTP"
            logging to zone
        exit
     exit
    commit
----------------------------------------------
*A:7705:Dut-A> config>security#
```

3.2.7.4 Fragmentation Handling

Security functionality on the 7705 SAR can process TCP/UDP packet fragments; however, the fragment containing the header must arrive first. If this condition is not met, the following actions occur.

- The firewall drops all fragmented packets arriving on the 7705 SAR until the fragment that contains the TCP/UDP header arrives.
- For bidirectional forwarding, packets arriving from the opposite direction are discarded because no session was created for the forward direction.
- For any TCP/UDP packets traversing from a public network to a private network and destined for a local IP address on the 7705 SAR, fragmented packets that do not contain the TCP/UDP header are extracted to the CSM for processing and an ICMP error message is sent to the sender.
- For destination NAT (port forwarding) packets traversing from a public network to a private network and destined for a local IP address on the 7705 SAR, fragmented packets that do not contain the TCP/UDP header are extracted to the CSM for processing and an ICMP error message is sent to the sender.

On the 7705 SAR-8 Shelf V2, 7705 SAR-18, and 7705 SAR-X, in addition to the condition requiring the fragment containing the header to arrive first, all fragments of a given packet must arrive on the same adapter card for processing.

If packets for an application such as DNS or ICMP are fragmented and the first fragment does not contain the information needed to make a firewall decision, the packet is discarded.

A security profile configured with strict TCP requires that all packets, including packet fragments, are extracted to the CSM for processing. The CSM checks for repeated packet fragments and discards them, and also checks the fragment offset to ensure that all fragments correspond to the correct offset.

3.2.8 Security Policies

Security policies define the rules within a zone that a packet must match in order for a defined action to be applied. Policies can vary from subscriber to subscriber and are applied to zones at the time the zone is created. The 7705 SAR supports the matching criteria and policy actions described in Table 10.

A security policy performs NAT when the policy entry is configured with the action to perform NAT and is configured with the destination IP address and port address parameters. NAT policies are all of type NPAT, meaning that they use both a network address translation and port address translation mechanism. Within a NAT policy, if the defined action is NAT, the packet has NAT applied to it based on the configured NAT pool IP address and ports.

Note: A security policy is a template that can be applied to multiple zones.

Table 10 **Security Policy Attributes and Packet Matching Criteria**

Attribute	Description	CLI Command
Action	Specifies how a packet is handled if a criterion is matched. If the zone finds a match for all the specified criteria, then it performs the specified actions on the packet. If there is no match, the packet is dropped. The supported policy actions are: • forward – a security session is created on the datapath with the action to forward the packets • reject – the packet is rejected after CSM extraction and examination, and no security session is created on the datapath (this is the default action and will occur as soon as a zone is created) • drop – a security session is created on the datapath with the action to drop the packets • nat – a NAT security session is created on the datapath, punching a hole through the firewall	action

Table 10 **Security Policy Attributes and Packet Matching Criteria (Continued)**

Attribute	Description	CLI Command
Packet flow direction	Specifies whether the policy matching criteria are applied to packets that are inbound to a zone, outbound from a zone, or to both inbound and outbound packets. The supported directions are zone-inbound, zone-outbound, or both. The **both** option does not apply to NAT.	direction
Match (protocol ID)	Specifies a protocol ID that the protocol specification of the packet must match	match
Source IP	Specifies an explicit source IP address for the match criteria of the rule. Packets being processed by a zone are evaluated for a match to the specified source IP address.	src-ip
Destination IP	Specifies an explicit destination IP address for the match criterion of the rule. Packets destined for the specified IP address are evaluated for a match.	dst-ip
Source Port	Specifies a source port to match in the IP packets when the match attribute is specified as protocol ID	src-port
Destination Port	Specifies a destination port to match in the IP packets when the match attribute is specified as protocol ID	dst-port
ICMP Code	Specifies the ICMP code when the protocol ID specified for the match attribute of the rule is set to ICMP	icmp-code
ICMP Type	Specifies the ICMP type when the protocol ID specified for the match attribute of the rule is set to ICMP	icmp-type
Profile	Specifies the profile ID applied to the policy	profile
Concurrent Sessions	Specifies the number of concurrent sessions that can be created using a single rule or zone	concurrent-sessions

3.2.9 Bypass Policies for a Firewall in a Layer 2 Service

Bypass policies for firewalls in a Layer 2 service allow certain traffic, such as control plane protocols (OSPF, RIP, BGP, IGMP, PIM, LDP, RSVP, VRRP, DHCP, NTP, and so on) to bypass a firewall in a Layer 2 service security zone. Bypass policies are configured with the **config>security>bypass** command. Each bypass policy that is created also uses one of the system's filter entry slots.

When processing protocol packets defined in the bypass policy, the 7705 SAR ignores the firewall lookup table, even if there is a more specific matching rule for the firewall. The bypass policy must be created carefully to ensure that it does not cause any security holes on the node.

If bypass policies are used on an upstream router, appropriate CPM filters should be configured on downstream nodes for the allowed or disallowed protocols.

If no bypass policy is configured, the protocol packets are firewalled based on the firewall rules.

3.2.10 Security Session Resource Alarms

The system monitors the overall session resource utilization. An alarm state is declared if the utilization exceeds the user-configurable high-water mark (**session-high-wmark**). The alarm condition is only cleared when the utilization has dropped below the user-configurable low-water mark (**session-low-wmark**).

If the thresholds are not configured, an alarm is raised if utilization reaches 100% and is cleared when utilization drops to 0%.

Session resource utilization alarms are described in Table 11.

Table 11 **Session Resource Utilization Alarms**

Event	Description	SNMP Notification
All security session resources have been exhausted	This event is generated if all session resources have been exhausted (utilization reaches 100%)	aluSecSessionsExhausted

Table 11 **Session Resource Utilization Alarms (Continued)**

Event	Description	SNMP Notification
Security session resource alarm detected	This event is generated when a resource alarm state is detected. The alarm state is detected when either the high-water mark is crossed (if configured) or all session resources have been exhausted.	aluSecSessionHiWtrMrkCrossed
Security session resource alarm cleared	This event is generated when a security session resource alarm state is cleared. This alarm state is cleared when either the low-water mark is crossed (if configured) or all sessions have been cleared.	aluSecSessionLoWtrMrkCrossed
Security session resource alarm threshold modified	This event is generated when the high or low thresholds for the alarm state are modified.	aluSecSessionWtrMrkModified

3.2.11 Security Logging

An essential component of security functionality is the ability to log events in order to have a view of the types of traffic and connections that are attempting to traverse a network. Events can be logged for each entry of a security policy or for a zone. Use the **config>security>logging** command to configure a logging profile, and then specify the log event or event type in the profile using the **event-control** command. For each event or event type, configure an action (one of **suppress**, **throttle**, or **off**) to determine how the event should be handled in the logging profile. To enable logging, the **logging** command must be configured in the security policy.

In addition to logging events per zone or per rule, the following can be logged:

- the permitted inbound or outbound security sessions that are destined for or traversing the 7705 SAR
- firewall administrative logs such as the number of policies or rules that have been created or deleted
- the dropped or rejected packets or sessions that are destined for or traversing the 7705 SAR

The 7705 SAR supports logging of the following firewall event types:

- packet events, described in Table 12
- zone events, described in Table 13
- policy events, described in Table 14
- session events, described in Table 15
- application events, described in Table 16
- ALG events, described in Table 17

Table 12 **Firewall Packet Events**

Event	Description
TcpInvalidHeader	The full TCP Header is not provided in the TCP segment.
DnsInvalidHeader	The format or content of the DNS packet is not valid. For example, the packet is a DNS answer from client to name server.
DnsUnmatchedAnswer	A DNS answer has been received without a preceding DNS query that matches the query ID.
IcmpUnmatchedReply	An ICMP response has been received without a preceding ICMP request that matches the ICMP request ID.
TcpInvalidFlagCombination	The TCP header contains flag combinations that are not valid and the packet may have been generated to probe the network or disrupt traffic.
TcpRst	A TCP RST has been generated with no matching session.
PolicyErrorFrag	The packet is a fragment and has been dropped; for example, because the first fragment received does not contain the entire protocol header, the reassembly time has expired, the limit on the number of non-adjacent fragments has been exceeded, or the fragment overlaps an existing fragment of this packet.
FragDropAction	The fragment packet has been rejected as the result of a problem with an earlier fragment of this packet.
DuplicateFrag	The fragment duplicates another fragment of this fragmented packet.
LandAttack	Source and destination IP addresses and UDP/TCP/SCTP ports all have the same value. This is an attack packet.

Table 13 **Firewall Zone Events**

Event	Description
NoRuleMatched	The packet is associated with a zone (source or destination) but does not match any rule in that zone.
SessionLimitReached	The configured limit of sessions for this IP protocol has been reached and this session cannot be established.

Table 14 **Firewall Security Policy Events**

Event	Description
Matched	A non-NAT rule has been matched in the creation of a session for this packet.
MatchedNAT	A NAT rule has been matched in the creation of a session for this packet.
ActionReject	A rule has been matched for this packet with the action to reject. The packet has been dropped and no session has been created.
MaxConcurrentUsesReached	A rule has been matched by this packet whose limit of concurrently active sessions has been exceeded. The rule has been skipped and an attempt to match a succeeding rule has been made. If no succeeding rule matches this packet, the packet is dropped and no session established.
FragsNotAccepted	The packet is fragmented and the matched rule does not allow fragments. The packet will be dropped and no session will be created.
TcpSynReqdtoEstablish	An invalid combination of TCP flags was encountered on a non-existent TCP session, so the packet was dropped.

Table 15 **Firewall Session Events**

Event	Description
InvalidIcmpT3	An ICMP packet type 3 packet is invalid. This may be due to policy configuration.
PktLimitReached	A security session has not been created because the zone-based session limits have been reached.

Table 15 **Firewall Session Events (Continued)**

Event	Description
ProhibitedIpOption	A packet with invalid or malformed IP options was encountered so it was dropped.
RuleActionDrop	Due to policy configuration, a drop session exists for the packet flow and all packets are discarded for the duration of the session.
SessionBegin	A new session has been created. The session may be a PASS or a DROP session and will continue to exist until the inter-packet interval configured for the session has been exceeded. Events such as a TCP full-close or TCP RST can also trigger the termination of the session.
SessionEnd	A session has terminated. This is either as the result of an operator action or the natural expiration of the session when the inter-packet interval has been exceeded.
SessionBeginEnd	The packet has been passed but the session allows only one packet and has been terminated. This can be accomplished by configuring an inter-packet interval of zero. Such sessions are sometimes used by an operator to pass ICMP type 3 notifications that do not match an existing session.

Table 16 **Firewall Application Events**

Event	Description
Summary	If TCP events have been discarded as a result of event-rate throttling, this event will identify the types of events that have been discarded.
HandshakeMissing	The TCP connection did not start with a SYN, SYN_ACK sequence.
HandshakeCtlInvalid	RST or ACK on SYN packet or data flags on dataless TCP SYN.
HandshakeDataUnexpected	The SYN packet has data in non-T/TCP handshake.
OptError	One or more TCP options are corrupted.
OptBadLen	A TCP option has an incorrect length.
OptTTcpForbidden	T/TCP options are present but not permitted.
OptNonStdForbidden	Experimental TCP options are present but not permitted.
OptTStampMissing	TCP timestamps have been negotiated but the timestamp option is not present.

Table 16 **Firewall Application Events (Continued)**

Event	Description
OptTStampUnexpected	The TCP timestamp is present but has not been negotiated.
TStampTooOld	The TCP timestamp value is too old.
TStampEchoInvalid	The echoed TCP timestamp is greater than expected.
ScaleUnexpected	The TCP scale option is present but has not been negotiated.
SeqNumOutside	The TCP sequence number is outside the window.
AckNumOutside	The TCP acknowledgment number is outside the window.
AckNumNotZero	There is no TCP ACK flag but the ACK number is not zero.
AckNumStale	An old TCP ACK flag is being used for a reused connection.
AckUnexpected	The TCP ACK flag is present but the connection has not yet synchronized.
AckMissing	The TCP ACK flag is expected but not present
FlagsSynRst	The TCP SYN and RST flags are both set.
SynUnexpected	The TCP SYN flag is present after the handshake completed.
SynMissing	The TCP SYN flag is not present but the connection has not yet synchronized.
FinUnexpected	There is a duplicate TCP FIN in this direction.
InvCksum	There is an invalid TCP checksum.
ConnReused	A TCP packet has been received on a closed connection
RstSeqNumUnexpected	The TCP RST sequence number is out of order.
TTL	The TCP TTL has been changed inappropriately.
NotFullHeader	The complete TCP header was not present.
FlagsSynFin	The TCP SYN and FIN flags are both set. Likely a probe or an attack.
SplitHandshake	The TCP SYN with no ACK was received when TCP SYN/ACK expected.

Table 17 **Firewall ALG Events**

Event	Description
CmdIncomplete	The ALG control session contained an incomplete command.
DynamicRuleInserted	A rule has been inserted into the rule list for a zone to permit a data session to be established.
DynamicRuleInsertedPASV	A rule has been inserted into the rule list for a zone to permit a data session to be established (PASV mode).
CannotInsertDynamicRule	This is an unusual event.
CannotInsertDynamicRulePASV	This is an unusual event.
BadCmdSyntax	The ALG control session contained an invalid command. The packet will be dropped.
BadPortCmdSyntax	The FTP control session contained an invalid TCP port specification. The packet will be dropped.
BadPasvCmdSyntax	The FTP control session contained an invalid PASV specification. The packet will be dropped.
BadAddrSyntax	The FTP control session contained an invalid IP address specification. The packet will be dropped.
TftpDynRuleInsertEr	This is an unusual event.
TftpDynRuleInserted	A rule has been inserted into the rule list for a zone to permit a TFTP data session to be established.

3.2.12 Firewall Debugging

If a security session is suspected of having a problem, it can be investigated with the firewall debugging capability. Use the **debug>security>capture** command to capture and isolate for inspection packets that are being processed by the firewall. Depending on the configured destination, packets are sent to a log or the console. The contents of the log can be viewed using the **show>security>capture** command.

To configure the capture capability, a zone identifier must be specified and the **start** command must be issued; however, every time a start command is issued, the contents of the log are cleared. The extraction rate for the capture capability is 25 packets/s. By default, the packet-capture process is continuous and packets are never dropped. However, when the log reaches 1024 packets, the oldest entry in the log is overwritten with a new one. Configuring the optional **count** *packets* parameter in the **start** command specifies the number of packets that will be captured before the oldest entry in the log is overwritten with a new one.

Note: It is recommended that the **debug>security>capture>start>count** *packets* option be used rather than continuous capture.

To stop the capture process, use the **debug>security>capture>stop** command. To view the configured packet-capture parameters, use the **show>debug** command.

3.2.13 NAT Security

Network Address Translation (NAT) is used by mobile backhaul, enterprise, and SI (Strategic Industries) providers to provide expandability and security for private networks. Tier 1 providers can potentially run out of private IPv4 addresses, making it difficult to expand their existing networks. To address this issue, NAT can be used. NAT can hide multiple private IP addresses behind a single public IP address and therefore makes it possible to scale IP solutions in mobile backhaul, enterprise, and SI networks.

For example, when applying NAT to a typical metrocell deployment, the cell site network is divided into two separate segments, a private domain and a public domain. Private domain network IP addressing needs to be hidden from the public domain. NAT makes all metrocells accessible via a single IP address visible in the public domain. The IPSec tunnels generated from metrocells are uniquely identified using IPSec NAT traversal (NAT-T).

Besides conserving available IPv4 addresses, NAT can also be used as a security feature to hide the real IP addresses of hosts, securely providing private LAN users access to public addresses.

This section describes security functionality specific to NAT, and covers the following topics:

- NAT Zones
- Dynamic Source NAT

- Local Traffic and NAT
- Port Forwarding (Static Destination NAT)
- Static One-to-One NAT

3.2.13.1 NAT Zones

With source NAT, a traffic session can only be initiated from a private domain to a public domain. Unless a session is created, packets from the public domain cannot be forwarded to the private domain. All arriving packets from the private domain, which are routed towards a public interface, are checked to determine if they traverse a NAT zone. If so, the packets are examined against the NAT policy rules. If there is a match between the policy and the packet, NAT is applied to the packet. Source NAT changes the source IP address and the source port of the packet, based on the configured NAT pool.

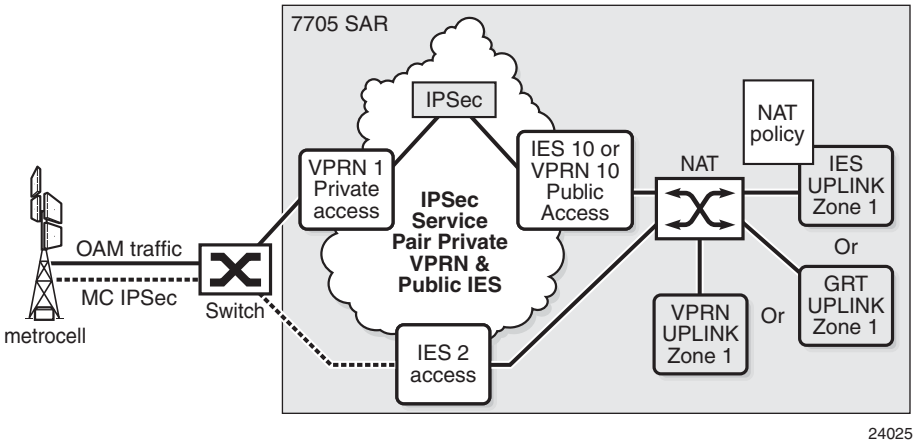
Zones can be segmented as small as a single interface or as large as the maximum number of interfaces supported by the 7705 SAR. For example, in metrocell applications, all the SAPs on the access point used to aggregate the metrocell can be placed in a single zone (zone 2) and the uplink public interface can be placed in another zone (zone 1). All traffic routed between the two zones uses NAT rules based on the NAT policies created for zone 1 and zone 2.

An example of the above zone configuration is shown in Figure 6.

Note:

- Zone 1 or zone 2 can be omitted if no specific security policy match criteria are required on the zone.
- If a packet does not travel between any zones, then NAT policies are not applied.

Figure 6 **Zone Configuration in a Mobile Backhaul Network**



In Figure 6, the OAM traffic from the metrocell is not encrypted. The OAM traffic is aggregated into a single VPRN service and IPSec functionality encrypts the OAM traffic. The encrypted traffic enters IES 10 or VPRN 10 with an IPSec header that has a routable IP destination address (typically to a security gateway) in addition to the encrypted payload. The far-end destination IP address can be reached through IES uplink zone 1, GRT uplink zone 1, or VPRN uplink zone 1. Since the traffic from IES 10 or VPRN 10 to the uplink zone crosses a zone boundary, the zone policy is applied to the uplink interface, and NAT is applied to the packet. The source IP address in the packet is replaced with the IP address of the uplink interface.

Similarly, in Figure 6, traffic from the metrocell (indicated by the dashed line), is encrypted by the metrocell with a valid IP header that contains a destination IP address (typically to a security gateway). The far-end destination is reachable through IES uplink zone 1, GRT uplink zone 1, or VPRN uplink zone 1. The packet has NAT applied to it because the packet must cross a zone boundary. The source IP address of the metrocell packet that enters IES 2 is replaced with the source IP address of IES uplink zone 1 as it exits the 7705 SAR. In addition, the source UDP/TCP port may also be replaced depending on the NAT policy configured for the zone.

In both of the cases described above, NAT is applied to the IP traffic according to NAT zone policy rules configured for IES uplink zone 1, GRT uplink zone 1, or VPRN uplink zone 1.

When using NAT in conjunction with IPSec, all IPSec tunnels must be configured (enabled) with NAT traversal (NAT-T) functionality. Enabling NAT-T on IPSec causes an insertion of the UDP port below the IPSec IP header. This UDP port can be used by NAT to uniquely identify each IPSec tunnel.

With static destination NAT, when packets from a public domain arrive at a zone, their source and destination IP addresses are evaluated to determine from which interface within the zone the packet will egress.

3.2.13.2 Dynamic Source NAT

Source NAT can be used to create sessions from inside a private network to an outside (public) network. If an arriving IP packet on the 7705 SAR matches the NAT policy rules, an internal mapping is created between the inside (private) source IP address/source port and an outside (public) source IP address/source port. The public IP address and port are configured in the NAT pool policy.

NAT automatically creates a reverse mapping for arriving traffic from the public domain to the private domain for the same connection. This reverse mapping is based on an outside destination IP address and destination port to an inside destination IP address and destination port.

The configurable outside NAT pool for the source IP address and source port can be either a range of addresses and ports or a unique IP address and port.

The 7705 SAR also supports a single public IP address so that all inside source IP addresses can be mapped to a single outside IP address and a range of ports. In this case, the interface name can be assigned to the NAT pool configuration. For ease of configuration, any local interfaces on the 7705 SAR can be assigned to the NAT pool (for example, local Layer 3 interfaces, loopback interfaces).

By assigning the Layer 3 interface name, the NAT pool inherits the IP address of that specific interface. For a DHCP client, the NAT pool IP address can change based on the IP address assigned to the interface by the DHCP server. If the interface IP address changes, all associated NAT sessions are cleared and re-established.

3.2.13.3 Local Traffic and NAT

Source NAT does not support self-generated traffic such as OSPF, BGP, or LDP.

Only packets transiting the 7705 SAR node have NAT applied to them. Any packet arriving on the 7705 SAR with a local IP address will be checked against active NAT sessions on the datapath (6-tuple lookup), and if there is no match, the packet is sent to the CSM for processing as local traffic.

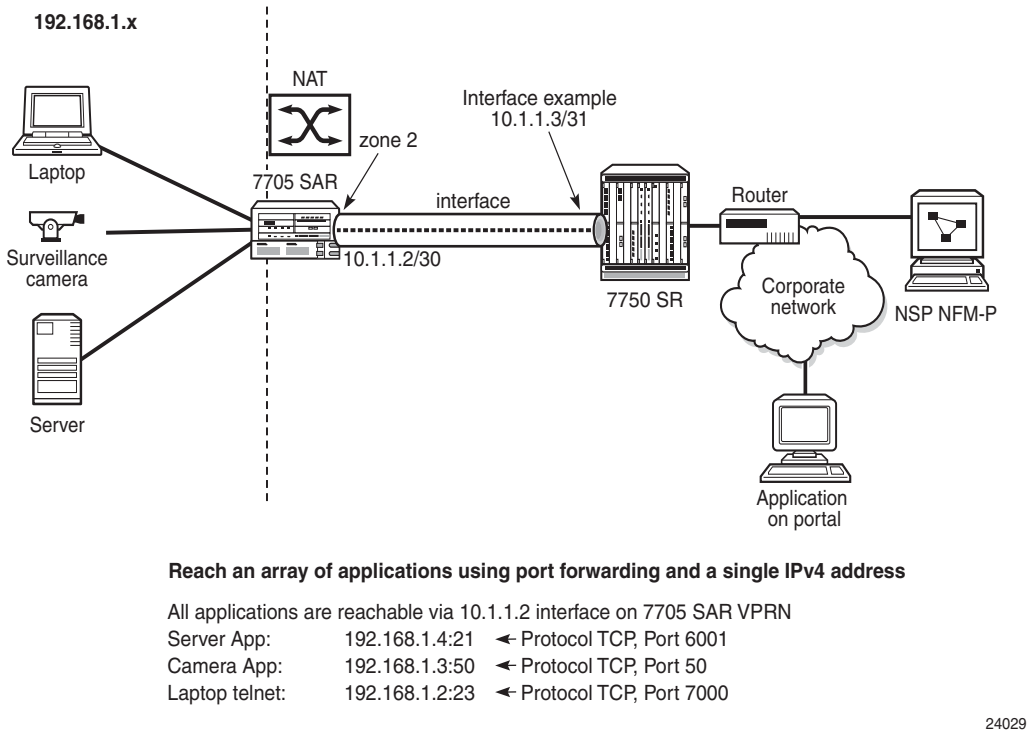
3.2.13.4 Port Forwarding (Static Destination NAT)

Port forwarding consists of mapping an outside destination port to an inside destination IP address and port. For example, a packet arriving from outside on port X and using a UDP protocol (from any IP address) is mapped to an inside destination port and destination IP address.

A typical use of port forwarding is shown in Figure 7. Each inside application is uniquely accessible via an outside port. For example, the surveillance camera behind the 7705 SAR can be reached via the UDP protocol and port 50. Any packet from any IP address arriving on destination port 50 is mapped to an internal destination IP address of 192.168.1.3 and destination port 50.

Caution: Using port forwarding for well-known ports can disrupt in-band local management traffic.

Figure 7 **Static Port Forwarding with NAT**



Static port forwarding can provide accessibility to applications behind a single IP address. Each application can be uniquely accessed via the public IP address and the destination port for that application.

Matching criteria for port forwarding includes local interface IP address, source IP address, and source UDP/TCP port.

3.2.13.5 Static One-to-One NAT

With static one-to-one NAT, NAT is performed on packets traveling from an inside (private) interface to an outside (public) interface or from an outside interface to an inside interface. Static one-to-one NAT can be applied to a single IP address or a subnet of IP addresses and is performed on the IP header of a packet, not on the UDP/TCP port.

Mapping statements, or entries, can be configured to map an IP address range to a specific IP address. The direction of the NAT mapping entry dictates whether NAT is performed on a packet source IP address or subnet or on a packet destination IP address or subnet. The 7705 SAR supports inside mapping entries that map an inside IP address range to an outside IP address range sequentially.

With an inside mapping entry, the following points apply.

- Packets that originate from an inside interface and are destined for an inside interface are forwarded without any NAT being applied.
- If there is a matching one-to-one NAT mapping entry, packets that originate from an inside interface and are destined for an outside interface undergo static one-to-one NAT where NAT changes the source IP address of the packet IP header. The packet is forwarded whether or not a NAT mapping entry is found unless the **drop-packets-without-nat-entry** command is enabled. When a mapping entry is not found and the **drop-packets-without-nat-entry** command is enabled, the packet is not forwarded.
- If there is a matching one-to-one NAT mapping entry, packets that originate from an outside interface and are destined for an inside interface undergo static one-to-one NAT where NAT changes the destination IP address of the packet IP header. The packet is forwarded whether or not a NAT mapping entry is found unless the **drop-packets-without-nat-entry** command is enabled. When a mapping entry is not found and the **drop-packets-without-nat-entry** command is enabled, the packet is not forwarded.
- Packets that originate from an outside interface and are destined for an outside interface are forwarded without any NAT being applied.

Static one-to-one NAT is performed on packets that transit the node and match the mapping entry. These packets include IPSec packets, GRE packets, and IP packets. NAT can be performed on packets from a single inside interface or multiple inside interfaces that are traveling to a single outside interface or multiple outside interfaces.

Static one-to-one NAT is not performed on packets that are destined for the node nor is it performed on self-generated traffic or on routing protocols. The 7705 SAR blocks static one-to-one NAT to a public prefix that has the same IP subnet as a local interface.

Static one-to-one NAT is supported in the GRT and in VPRNs. For information about VPRNs and one-to-one NAT, refer to the 7705 SAR Services Guide, “Static One-to-One NAT and VPRN”.

Table 18 lists the types of outside and inside interfaces that are supported in the GRT for static one-to-one NAT.

Table 18 **GRT Interfaces Supported for Static One-to-One NAT**

GRT Interface Type	Outside	Inside
Network interface	Yes	No
IES interface	Yes	Yes
IES r-VPLS interface	Yes	Yes
IES Layer 3 spoke SDP interface	Yes	Yes
IPSec public interface	n/a	n/a

3.2.13.5.1 Static One-to-One NAT and ICMP

Typically, the original packet in a flow is embedded in an ICMP Error packet. When static one-to-one NAT is configured, the payload of the ICMP Error packet is modified based on the NAT mapping.

3.2.13.5.2 Static One-to-One NAT and FTP

Static one-to-one NAT does not modify the IP address of FTP control packets.

3.2.13.5.3 Static One-to-One NAT and Firewall Security

Static one-to-one NAT and firewall security zones can be configured simultaneously. A firewall zone can include static one-to-one NAT inside interfaces or static one-to-one NAT outside interfaces. However, when a firewall security policy is used by a firewall zone, any IP address referenced in the policy must be based on the inside addressing scheme if the address involves NAT mapping, regardless of whether the interface under the firewall zone is a one-to-one NAT inside interface or outside interface.

3.2.13.5.4 Static One-to-one NAT and NPAT

Static one-to-one NAT and network port address translation (NPAT) cannot coexist within the same routing instance. However, they can coexist in an IPSec configuration when static one-to-one NAT is configured for the IPSec private service and NPAT is configured for an IPSec public service that is enabled with NAT-T.

3.2.13.5.5 Static One-to-One NAT Route Leaking to IGP or BGP

Static one-to-one NAT installs NAT routes in the routing table. By default, these routes are not advertised to the network. For example, if a user configures a NAT mapping entry that is not using a local interface IP address as its public NAT prefix, the NAT routes will be installed in the routing table but are not advertised to the network. For these routes, route policies can be used to leak one-to-one NAT routes to IGP or BGP.

Proxy ARP can be used to resolve the MAC addresses of these non-local NAT routes.

3.2.13.5.6 PBR and MFC

Both policy-based routing (PBR) and multi-field classification (MFC) are available when static one-to-one NAT is configured. PBR and MFC are applied to packets before the packets undergo NAT.

3.2.13.5.7 Cflowd and Mirroring

When static one-to-one NAT is configured, the original packets received on ingress will be used for Cflowd and the transformed packets sent on egress will be shown for mirroring.

3.2.13.5.8 Private IP Address Ping, Traceroute, and Packet Forwarding

When static one-to-one NAT is configured, if a packet arrives on an outside interface and is destined for an inside IP address, it is not forwarded to the inside IP address; instead, it is dropped.

Similarly, if a ping or traceroute packet arrives from an outside interface and is destined for an inside IP address, the packet is not forwarded for security reasons.

It is recommended that operators set up ingress ACLs and security zones on the outside interface to ensure full security of the inside network.

3.2.13.5.9 Fragmentation

The 7705 SAR supports static one-to-one NAT for fragmented packets.

3.2.14 Multi-Chassis Firewall

Multi-chassis firewall synchronizes firewall and NAT states between two 7705 SAR routers. Both routers can have traffic traversing them, but they create a single firewall-and-NAT database on one router, known as the master. That database is synchronized and shared with the second router, known as the slave. If one firewall in a multi-chassis firewall fails, all the known UDP/TCP sessions and states are present on the other chassis. The connection can therefore continue transmitting traffic on a 5-tuple session without re-establishing the state of the session. For example, if there is a TCP connection on the first firewall that has gone through the three states of TCP, that information is synchronized to the second firewall. If there is a failure on the first firewall where the session originally was established and the traffic gets rerouted to the second firewall in the pair, the second firewall can forward the traffic on the same TCP connection without any interruption because it knows the state of the connection.

Multi-chassis firewall is supported on the following cards and platforms:

- on the 7705 SAR-8 Shelf V2 and the 7705 SAR-18:
  - 2-port 10GigE (Ethernet) Adapter card
  - 6-port Ethernet 10Gbps Adapter card
  - 8-port Gigabit Ethernet Adapter card, version 3
  - 10-port 1GigE/1-port 10GigE X-Adapter card, version 2 (7705 SAR-18 only)
- 7705 SAR-Ax
- 7705 SAR-H
- 7705 SAR-Hc
- 7705 SAR-Wx
- 7705 SAR-X

Note: The two routers used in a multi-chassis firewall configuration must be the same. Different platforms will not synchronize.

All GRT and VPRN-based firewall functionality is supported in multi-chassis mode except for strict TCP and ALG. As well, in order for NAT to work in multi-chassis firewall and to have the same NAT state between the two firewalls, a loopback interface must be used. See Multi-Chassis NAT for more information.

The 7705 SAR uses a multi-chassis link (MCL) to connect the two firewalls in a multi-chassis configuration. The MCL must be a static route to the peer IP address.

The parameters that define the MCL are configured in the **config>redundancy>multi-chassis>peer>mc-firewall** context. Refer to “High Availability (Redundancy) Commands” in the 7705 SAR Basic System Configuration Guide for command descriptions and syntax.

Note: A dedicated port should be assigned for multi-chassis firewall communication. This will ensure that any failure on the datapath ports will not affect the multi-chassis firewall communication. A redundant link should also be assigned for multi-chassis firewall communication in case of port or fiber failure.

3.2.14.1 Multi-Chassis Firewall Configuration

The steps below outline how to configure a multi-chassis firewall.

Step 1. On both routers, configure security profile, security policy, host group, and application group parameters. The parameter settings must be identical on both routers. See Security Policy Commands for information on configuring these parameters.

Step 2. On both routers, configure identical security zone parameters so that the routers have the same zone ID on the same service ID and service type, the same NAT pool settings, and the same zone limits for inbound and outbound firewall sessions. The service ID and service type apply only to security zone configuration in the VPRN or IES context. For information on configuring security zone parameters in the VPRN context or in the IES context, refer to “VPRN Security Zone Configuration Commands” or “IES Security Zone Configuration Commands” in the 7705 SAR Services Guide. For information on configuring security zone parameters in the base router context, see Router Security Zone Configuration Commands.

Step 3. On both routers, configure the multi-chassis firewall by configuring the following multi-chassis firewall peer parameters: the peer IP address, the system priority, and optional encryption or authentication parameters. For information on configuring these parameters, refer to “High Availability (Redundancy) Commands” in the 7705 SAR Basic System Configuration Guide.

Step 4. On both routers, issue the **config>redundancy>multi-chassis>peer>mc-firewall>no shutdown** command to initiate communication between the peers and enable the master and slave selection. For more information on master and slave, see Multi-Chassis Firewall Master/Slave Selection and Policy and Session Database Synchronization.

Step 5. Issue the **admin save** command on each router to save the configuration.

3.2.14.2 Multi-Chassis Firewall Master/Slave Selection and Policy and Session Database Synchronization

Determining which router will be the master and which will be the slave is based on the system priority configured using the **config>redundancy>multi-chassis>peer>mc-firewall>system-priority** command. The router configured with the lower system priority becomes the master. If both routers have the same system priority, the router with the lowest MAC address becomes the master.

When the MCL is established and the master and slave routers are determined, the master router synchronizes its security policy configuration to the slave router over the MCL. This synchronization overwrites any security policy configuration on the slave.

In addition, the master synchronizes its session database to the slave. This synchronization is for all established security and NAT sessions. The master does not synchronize any half-open sessions to the slave. This synchronization overwrites the session database on the slave.

If policy synchronization fails, all security sessions are terminated and the security policy configuration on the slave router will be in an incomplete state. A policy synchronization flag on the master remains cleared until synchronization resumes. When synchronization completes, the policy synchronization flag changes to set. A corresponding log event is raised on the master router when the policy synchronization flag changes state.

Security zone and NAT pool information is not synchronized from the master to the slave. These parameters must be configured with identical settings on each router.

Note: It is recommended that any **system-priority** changes be performed during a maintenance window. If the system priority of a router changes, the master and slave negotiation will restart. The master router will synchronize its firewall security policy configuration and firewall database states to the slave, overwriting the existing firewall security policy configurations and database states on the slave.

3.2.14.3 Processing New Traffic Signatures and Connections on a Multi-Chassis Firewall

When the firewall database between the master and slave has been synchronized, the firewalls on both routers can process existing connections and signatures for arriving packets. However, the master firewall must create a datapath signature in the firewall database for each new connection.

If there is no datapath firewall database, all traffic from both the slave and master router is forwarded to the CSM on the master router. The slave router forwards its packets to the master CSM over the MCL. The master CSM examines the packet against the firewall security policy and creates a 5-tuple signature including the action (drop or forward).

This signature is downloaded to the datapath firewall database on the master and to the datapath firewall database on the slave over the MCL. From this point on, both the master and slave have the packet signature and action in their datapath firewall database.

3.2.14.4 Adding, Modifying, and Deleting a Firewall Security Policy in a Multi-Chassis Firewall

The steps below outline how to add a new firewall security policy or modify an existing one in a multi-chassis firewall configuration.

Step 1. On the master router, use the **begin** command to start an editing session.

Step 2. In the **config>security** context, configure settings for security **profile**, **host-group**, **app-group**, and/or **policy** (rule) commands on the master router.

Step 3. When the changes are complete, issue the **commit** command on the master router to save the policy settings.

The configuration is automatically synchronized to the slave router.

Step 4. Issue the **admin save** command on the master and slave routers to save the configuration.

The steps below outline how to delete a firewall security policy in a multi-chassis firewall configuration.

Step 1. Ensure that the policy is not being used by a zone on either the master or slave router.

Step 2. On the master router, use the **begin** command to start an editing session.

Step 3. Delete a policy from the master router using the **config>security>no policy** *policy-id* | *policy-name* command.

Step 4. When the policy is deleted, issue the **commit** command on the master router to save the change.

The change is automatically synchronized to the slave router.

Step 5. Issue the **admin save** command on the master and slave routers to save the configuration.

3.2.14.5 Adding, Modifying, and Deleting a Zone in a Multi-Chassis Firewall

In a multi-chassis firewall, zone configuration is not synchronized between the master and slave routers. All zone-level configuration, including the addition and deletion of zones, must be performed on each router separately.

The master and slave routers identify zones based on their assigned zone IDs. In the VPRN and IES service contexts, zone IDs must match and be assigned to the same service ID and service type on both the master and the slave routers. In all contexts (baser router, IES, and VPRN), all zone parameter configurations must match on both routers, except for the assigned interfaces.

Caution: Any changes to a zone configuration will affect service across all zones on the slave router. This operation should be performed only during scheduled maintenance.

3.2.14.5.1 Adding a Zone

The steps below outline how to add a new zone in a multi-chassis firewall configuration.

Step 1. On the master and slave routers, disable the multi-chassis peer using the **config>redundancy>multi-chassis>peer>mc-firewall>shutdown** command.

Step 2. On the master and slave routers, create a new zone.

In the base router context, use the **config>router>zone** *zone-id* | *zone-name* **create** command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone** {*zone-id* | *name*} [**create**] command.

Step 3. On the master and slave routers, put the new zone into a draft state.

In the base router context, use the **config>router>zone** *zone-id* | *zone-name* **begin** command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone** {*zone-id* | *name*} **begin** command.

Step 4. On the master and slave routers, assign a corresponding interface to the new zone.

In the base router context, use the **config>router>zone>interface** *interface-name* command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone>interface** *interface-name* command.

Step 5. On the master and slave routers, assign a policy to the new zone.

In the base router context, use the **config>router>zone>policy** *policy-id* | *policy-name* command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone>policy** *policy-id* | *policy-name* command.

The policy-to-zone assignment on the two routers must match.

Step 6. When changes are complete, save the changes on each router.

In the base router context, use the **config>router>zone** *zone-id* | *zone-name* **commit** command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone** {*zone-id* | *name*} **commit** command.

Step 7. On the master and slave routers, enable the multi-chassis peer using the **config>redundancy>multi-chassis>peer>mc-firewall>no shutdown** command.

Step 8. Issue the **admin save** command on the master and slave routers to save the configuration.

3.2.14.5.2 Modifying a Zone

The steps below outline how to modify a zone in a multi-chassis firewall configuration.

Step 1. On the master and slave routers, disable the multi-chassis peer using the **config>redundancy>multi-chassis>peer>mc-firewall>shutdown** command.

Step 2. On the master and slave routers, put the zone into a draft state.

In the base router context, use the **config>router>zone** *zone-id* | *zone-name* **begin** command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone** {*zone-id* | *name*} **begin** command.

Step 3. On the master and slave routers, change the zone interface, inbound and outbound limit parameters, NAT pool parameters, and/or policy-to-zone assignment.

Step 4. When changes are complete, save the changes on each router.

In the base router context, use the **config>router>zone** *zone-id* | *zone-name* **commit** command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone** {*zone-id* | *name*} **commit** command.

Step 5. On the master and slave routers, enable the multi-chassis peer using the **config>redundancy>multi-chassis>peer>mc-firewall>no shutdown** command.

Step 6. Issue the **admin save** command on the master and slave routers to save the configuration.

3.2.14.5.3 Deleting a Zone

The steps below outline how to delete a zone in a multi-chassis firewall configuration.

Step 1. On the master and slave routers, disable the multi-chassis peer using the **config>redundancy>multi-chassis>peer>mc-firewall>shutdown** command.

Step 2. On the master and slave routers, put the zone into a draft state.

In the base router context, use the **config>router>zone** *zone-id* | *zone-name* **begin** command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone** {*zone-id* | *name*} **begin** command.

Step 3. On the master and slave routers, remove the policy-to-zone assignment.

In the base router context, use the **config>router>zone>no policy** command.

In the VPRN or IES context, use the **config>service>vprn | ies>zone>no policy** command.

Step 4. When changes are complete, save the changes on each router.

In the base router context, use the **config>router>zone** *zone-id* | *zone-name* **commit** command.

In the VPRN or IES contexts, use the **config>service>vprn | ies>zone** {*zone-id* | *name*} **commit** command.

Step 5. On the master and slave routers, delete the zone.

In the base router context, use the **config>router>no zone** *zone-id* | *zone-name* command.

In the VPRN or IES context, use the **config>service>vprn | ies>no zone** *zone-id* | *zone-name* command.

Step 6. On the master and slave routers, enable the multi-chassis peer using the **config>redundancy>multi-chassis>peer>mc-firewall>no shutdown** command.

Step 7. Issue the **admin save** command on the master and slave routers to save the configuration.

3.2.14.6 Multi-Chassis Firewall Security Logging

Security logging parameters and settings must match on the master and slave routers. To configure logging for each entry of a security policy or for a zone, the policy and zone must be put into a draft state using the **begin** command. When the changes are complete, the **commit** command must be used to save them to the firewall database.

If a multi-chassis firewall activity switch occurs, the existing security sessions on the new master router do not retain their logging attributes. Instead, new sessions that are established after the switch will assume the configured logging attributes.

On the CLI, security session status, timers, and details are shown only for the master. Session statistics for each 5-tuple signature are shown on both the master and slave.

3.2.14.7 MCL Failure

If the MCL goes down between the two firewalls for any reason, the two firewalls will function as standalone firewalls. They will each learn and process new connections arriving on the firewall, compare the connections against their own CSM firewall security policies, and program their respective databases accordingly.

When the MCL is re-established, the slave firewall will become synchronized to the master firewall. Previously learned signatures and previously provisioned configurations on the slave are overwritten with those on the master firewall.

Note: It is recommended that redundant MCLs be configured between the master and slave routers in a multi-chassis firewall configuration.

3.2.14.8 Multi-Chassis NAT

Only source NAT is supported in multi-chassis firewall configuration. For NAT to function correctly, a loopback address with the same IP address must be created on both firewall routers.This IP address should be in the NAT pool for source NAT so that return traffic can be routed to either router and undergo reverse NAT at either firewall. Proxy ARP can be created for this loopback address. See Proxy ARP for information.

3.2.14.9 MCL Encryption

The multi-chassis firewall messages on the MCL between the master and slave can be encrypted and authenticated. Encryption and authentication are important on this link in order to avoid man-in-the-middle attacks where hackers can insert signature packets and create new unwanted states in the firewall. The MCL is encrypted using the **config>redundancy>multi-chassis>peer>mc-firewall>encryption** command.

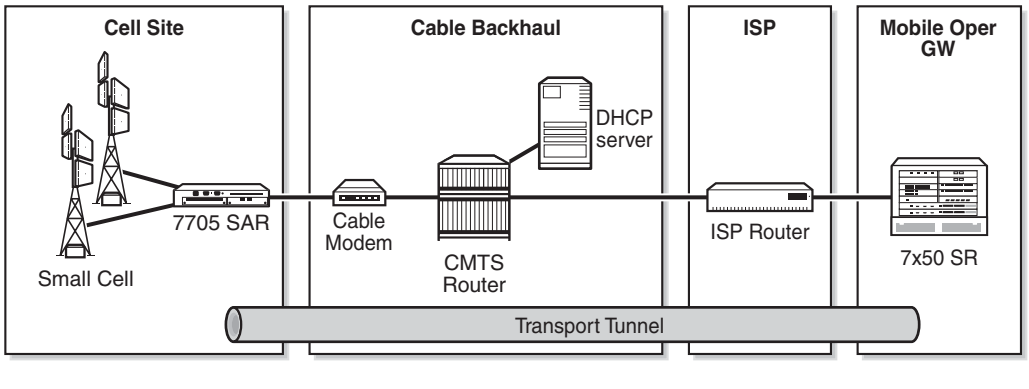
The 7705 SAR supports AES128 and AED256 encryption algorithms and SHA256 and SHA512 authentication algorithms.

A security association (SA) contains the keys that are required to encrypt and authenticate the link. A security association is uniquely identified by a security parameter index (SPI).There are two SPIs for key rollover. On egress, only the active outbound SA is used for encryption and authentication.The **active-outbound-sa** *num* command identifies the active SA, where *num* is the SPI for that SA. On ingress, decryption is done using both SPIs. Using both SPIs means that packets can be decrypted using the current and previous keys, allowing for a smooth transition.

3.3 Using the 7705 SAR as Residential or Business CPE

The 7705 SAR can be used as a residential or business CPE device for the purposes of ISP backhaul. With GPON, DSL, or cable-based residential or business backhaul services, specifically, ISPs typically terminate subscribers on a broadband network gateway to assign IP addresses, and to enforce authentication, authorization, and accounting before the customer traffic is routed for Internet access. By making use of the 7705 SAR as a CPE device, ISP backhaul infrastructure can be used to connect an eNodeB, such as a voice-free metrocell, to a network. The 7705 SAR continues to support a wide array of services, including IP-VPN, Ethernet, TDM, PWs, and VPLS services, over this backhaul by making use of GRE or IP tunnels. An example of a network using a 7705 SAR as a CPE device is shown in Figure 8.

Figure 8 **Network Using 7705 SAR as a CPE Device**



Residential or business CPE functionality is available through the use of:

- unnumbered interfaces

  In normal operation, the 7705 SAR requires at least two IP addresses: a system IP address and an uplink interface IP address. However, ISPs typically assign a single IP address per connection for residential or business backhaul services, due to cost or architectural issues. Configuring the 7705 SAR to use unnumbered interfaces alleviates this issue.

  See Unnumbered Interfaces for more information.

- dynamic assignment of system IP addresses through DHCP

  A 7705 SAR using unnumbered interfaces does not have a configured uplink interface IP address, as the uplink interface identifier is tied to the system IP address. In residential and business backhaul, the system IP address must be assigned dynamically. The system IP address can be assigned dynamically using DHCP when the 7705 SAR is acting as a DHCP client and the DHCP server-facing interface is unnumbered.

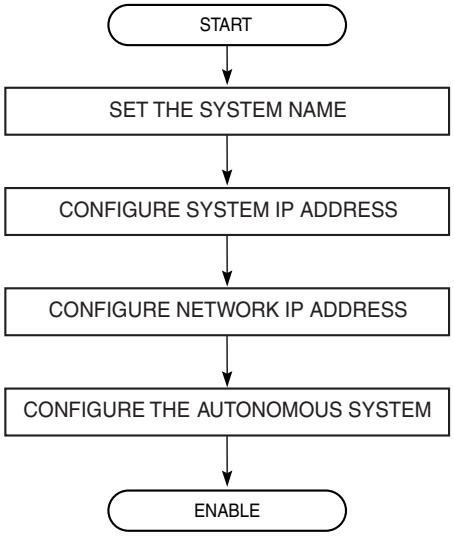
- automatic provisioning of a default gateway

  As part of a DHCP OFFER message, the ISP also offers a default gateway IP address to the client. The 7705 SAR, as the client, must set up a default route pointing to the default gateway once the gateway IP is offered via Option 3. The default gateway points to the network interface, which, as the DHCP server-facing interface, is unnumbered.

3.4 Router Configuration Process Overview

Figure 9 displays the process to configure basic router parameters.

Figure 9 **IP Router Configuration Flow**



3.5 Configuration Notes

The following information describes router configuration guidelines and caveats.

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

3.5.1 Reference Sources

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

3.6 Configuring an IP Router with CLI

This section provides information to configure an IP router.

Topics in this section include:

- Router Configuration Overview
- Basic Configuration
- Common Configuration Tasks
- Service Management Tasks

3.7 Router Configuration Overview

On a 7705 SAR, an interface is a logical named entity. An interface is created by specifying an interface name under the **config>router** context, the global router configuration context where objects like static routes and dynamic routing are defined. An IP interface name can be up to 32 alphanumeric characters, 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 a 7705 SAR, the basic configuration tasks that must be performed are:

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

A system interface and network interface should both be configured unless the network interface is configured as an unnumbered interface. In that case, the network interface borrows (or links to) an IP address from another interface on the system (the system IP address, another loopback interface, or any other numbered interface), which serves as a combined system IP address and network IP address.

3.7.1 System Interface

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

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

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

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

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

3.7.2 Network Interface

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

On the 2-port 10GigE (Ethernet) Adapter card/module, the network interface can only be created on the v-port (not the ring ports).

3.8 Basic Configuration

Note: Refer to Filter Policies and Route Policies for information on configuring these policies.

The most basic router configuration must have the following:

- system name
- system address

The following example displays a router configuration.

```
ALU-1>config>router# info
#------------------------------------------
# Router Configuration
#------------------------------------------
    router
        interface "system"
            address 192.0.2.1/24
        exit
        interface "to-104"
            address 192.0.2.1/24
            port 1/1/1
            exit
        exit
#------------------------------------------
A:ALU-1>config#
```

3.9 Common Configuration Tasks

The following sections describe basic system tasks:

- Configuring a System Name
- Configuring Router IPv6 Neighbor Discovery Parameters
- Configuring Interfaces
- Configuring IPv6 Parameters
- Configuring Router Advertisement
- Configuring ECMP
- Configuring Static Routes
- Configuring or Deriving a Router ID
- Configuring an Autonomous System
- Configuring ICMP and ICMPv6
- Configuring a DHCP Relay Agent
- Configuring Proxy ARP
- Configuring a Security Zone
- Configuring Security Logging
- Applying an Application Group and a Host Group to a Security Policy
- Configuring an IP Reassembly Profile

3.9.1 Configuring a System Name

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

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

Use the following CLI syntax to configure the system name:

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

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

The following example displays the system name output.

```
A:ALU-A>config>system# info
#------------------------------------------
# System Configuration
#------------------------------------------
        name "NOK-A"
        location "Kanata, ON, Canada"
        snmp
        exit
        . . .
        exit
-------------------------------------------
```

3.9.2 Configuring Router IPv6 Neighbor Discovery Parameters

Use the following CLI syntax to configure IPv6 neighbor discovery parameters:

CLI Syntax:

```
config# router
   ipv6
      reachable-time seconds
      stale-time seconds
```

Example:

```
config# router
config>router# ipv6
config>router>ipv6# reachable-time 30
config>router>ipv6# stale-time 14400
config>router>ipv6# exit
config>router# exit
```

The following example displays IPv6 neighbor discovery parameters output.

```
A:ALU-A>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
        ...
            reachable-time 30
            stale-time 14400
        exit
        ...
```

3.9.3 Configuring Interfaces

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

The system interface cannot be deleted.

3.9.3.1 Configuring a System Interface

Use the following CLI syntax to configure a system interface:

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

Example:
```
config>router# interface "system"
config>router>if# address 192.168.0.0/16
config>router>if# exit
```

3.9.3.2 Configuring a Network Interface

On the 2-port 10GigE (Ethernet) Adapter card/module, a network address is assigned to the v-port only.

Use the following CLI syntax to configure a network interface:

CLI Syntax:
```
config>router
   interface ip-int-name
      address {ip-addr/mask-length | ip-addr/netmask |
         dhcp} [client-identifier [ascii-value |
         interface-name]] [vendor-class-id vendor-class-
         id]
      egress
         agg-rate-limit agg-rate [cir cir-rate]
         filter ip ip-filter-id
         queue-policy name
      ingress
         filter ip ip-filter-id
      port port-name
```

Example:
```
config>router> interface "to-NOK-2"
config>router>if# address 192.168.0.1/16
config>router>if# port 1/1/1
config>router>if# egress
config>router>if>egress# filter ip 12
config>router>if>egress# exit
config>router>if# ingress
config>router>if>ingress# filter ip 10
config>router>if>ingress# exit
config>router>if# exit
```

The preceding syntax example shows a configuration where the address is entered manually. To have the interface enabled for dynamic address assignment, use the **dhcp** keyword and, optionally, assign client ID and vendor class ID.

In addition, to apply and configure a per-VLAN network egress aggregate shaper, use the **queue-policy** and **agg-rate-limit** commands.

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

```
A:ALU-A>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
        interface "system"
            address 192.168.0.0/16
        exit
        interface "to-NOK-2"
            address 192.168.0.1/16
            port 1/1/1
            ingress
                filter ip 10
            exit
```

3.9.3.2.1 Creating an IPv6 Network Interface

When configuring an IPv6 interface, a link-local address (fe80::x:x:x:x:x:x:x/64) is automatically generated after the CLI command **ipv6** is given. If the port is already assigned to the interface when IPv6 is enabled, the link-local address is derived from the port MAC address. Otherwise, the link-local address is derived from the system MAC address.

In either case, if the configuration file is saved and the node is rebooted, the port will be assigned to the interface before IPv6 is enabled and the link-local address will be derived from the port MAC address. This means that the link-local address will change after the node is rebooted if it was derived from the system MAC address before the reboot.

To avoid having the link-local address change after a reboot, IPv6 on the interface should be configured in the following order. This will ensure that the link-local address is derived from the port MAC address and will therefore not change after a reboot.

CLI Syntax:
```
config>port
config>router
   interface ip-int-name
      port port-name
      ipv6
         address ipv6-address/prefix-length
            [eui-64]
```

Note: A link-local address can also be manually configured with the **config>router>interface>ipv6>link-local-address** command. The manually configured link-local address overwrites the automatically generated address.

3.9.3.3 Configuring an Unnumbered Interface

Use the following CLI syntax to configure an unnumbered interface:

CLI Syntax:
```
config>router
   interface ip-int-name
      unnumbered [ip-int-name | ip-address] [dhcp]
         [client-identifier ascii-value | interface-name]
         [vendor-class-id vendor-class-id]
```

Example:
```
config>router> interface "to-NOK-3"
config>router>if# unnumbered "system"
config>router>if# exit
```

The preceding syntax example shows a configuration where the address is entered manually. To have the interface enabled for dynamic assignment of the system IP address, use the **dhcp** keyword and, optionally, assign client ID and vendor class ID.

3.9.4 Configuring IPv6 Parameters

IP version 6 (IPv6) addresses are supported on:

- access ports (IES); for a complete list of cards and ports that support IES IPv6 SAPs, refer to the 7705 SAR Services Guide, “IES for Customer Traffic”.

- network ports (null or dot1q encapsulation) on:
  - 2-port 10GigE (Ethernet) Adapter card (v-port only)
  - 8-port Ethernet Adapter card
  - 6-port Ethernet 10Gbps Adapter card
  - 8-port Gigabit Ethernet Adapter card
  - 10-port 1GigE/1-port 10GigE X-Adapter card
  - Packet Microwave Adapter card
  - Ethernet ports on the 7705 SAR-M
  - Ethernet ports on the 7705 SAR-A
  - Ethernet ports on the 7705 SAR-Ax
  - 7705 SAR-W
  - Ethernet ports on the 7705 SAR-Wx
  - 7705 SAR-H
  - Ethernet ports on the 7705 SAR-Hc
  - Ethernet ports on the 7705 SAR-X
  - Ethernet management port
  - 2-port 10GigE (Ethernet) module (v-port only)
  - 4-port SAR-H Fast Ethernet module
  - 6-port SAR-M Ethernet module
- network ports on the 4-port OC3/STM1 Clear Channel Adapter card (POS encapsulation)

Use the following CLI syntax to configure IPv6 parameters:

CLI Syntax:

```
config>router
   interface ip-int-name
      ipv6
         address ipv6-address/prefix-length [eui-64]
         bfd transmit-interval [receive receive-interval]
            [multiplier multiplier] [type np]
         icmp6 (see Configuring ICMP and ICMPv6)
         neighbor ipv6-address mac-address
         reachable-time seconds
         stale-time seconds
```

Example:

```
config>router# interface "ipv6-interface"
config>router>if# ipv6
config>router>if>ipv6>address# ip 2001:db8::1/32
config>router>if>ipv6>address# exit
config>router>if>ipv6# bfd 100 receive 100 multiplier 3
 type np
```

```
config>router>if>ipv6>bfd# exit
config>router>if>ipv6# neighbor 2001:db8::2
config>router>if>ipv6>neighbor# exit
config>router>if>ipv6# reachable-time 30
config>router>if>ipv6# stale-time 14400
config>router>if>ipv6# exit
```

3.9.5 Configuring Router Advertisement

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

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

CLI Syntax:

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

Example:

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

The following example displays a router advertisement configuration:

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

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

3.9.6 Configuring ECMP

ECMP (Equal-Cost Multipath Protocol) refers to the distribution of packets over two or more outgoing links that share the same routing cost. The 7705 SAR load-balances traffic over multiple equal-cost links with a hashing algorithm that may use header fields from incoming packets to calculate which link to use. Adding additional fields to the algorithm increases the randomness of the results and ensures a more even distribution of packets across available links. ECMP is supported on static routes and dynamic (OSPF, IS-IS, and BGP) routes. The 7705 SAR supports ECMP for LDP and IP traffic.

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

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

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

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

3.9.7 Configuring Static Routes

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

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

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

Use the following CLI syntax to create a static route entry. The **mcast** keyword indicates that the static route entry being configured is used for the multicast table only. The **black-hole**, **indirect**, and **next-hop** commands provide access to configure their parameters. Unless **no shutdown** is specified, the **static-route-entry** will be created in a **shutdown** state.

CLI Syntax:

```
config>router>
   static-route-entry {ip-prefix/prefix-length} [mcast]
      black-hole {ip-int-name | ip-address | ipv6-
         address}
         [no] description description-string
         [no] metric metric
         [no] preference preference
         [no] shutdown
         [no] tag tag
      indirect [ip-address]
         [no] description description-string
         [no] metric metric
         [no] preference preference
         [no] shutdown
         [no] tag tag
         tunnel-next-hop
            [no] disallow-igp
            resolution {any | disabled | filter}
            resolution-filter
               [no] ldp
               [no] rsvp-te
                  [no] lsp lsp-name
               [no] sr-isis
               [no] sr-ospf
               [no] sr-te
                  [no] lsp lsp-name
      next-hop {ip-int-name | ip-address | ipv6-address}
         [no] bfd-enable
         [no] description description-string
         [no] ldp-sync
         [no] metric metric
         [no] preference preference
```

```
[no] shutdown
[no] tag tag
```

Example:
```
config>router# static-route-entry 192.168.0.10/16
   static-route-entry# next-hop 192.168.0.20
      next-hop# metric 1
      next-hop# preference 5
      next-hop# ldp-sync
      next-hop# tag 20
      next-hop# no shutdown
```

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

3.9.8 Configuring or Deriving a Router ID

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

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

Use the following CLI syntax to configure a router ID:

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

The following example displays a router ID configuration:

```
A:ALU-B>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
        interface "system"
            address 192.168.0.10/16
        exit
        interface "to-103"
            address 192.168.0.20/16
            port 1/1/1
```

```
        exit
        router-id 192.168.0.0
...
#------------------------------------------
A:ALU-B>config>router#
```

3.9.9 Configuring an Autonomous System

Configuring an autonomous system is optional.

Use the following CLI syntax to configure an autonomous system:

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

The following displays an autonomous system configuration example:

```
A;ALU-B>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
     interface "system"
          address 192.168.0.10/16
     exit
     interface "to-104"
          address 192.168.0.30/16
          port 1/1/1
     exit
     exit
     autonomous-system 100
     router-id 192.168.0.1
#------------------------------------------
```

3.9.10 Configuring ICMP and ICMPv6

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

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

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

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

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

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

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

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

3.9.11 Configuring a DHCP Relay Agent

Use the following CLI syntax to configure the router as a DHCP Relay agent:

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

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

The following example displays the router DHCP Relay agent creation output.

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

3.9.12 Configuring Proxy ARP

To configure proxy ARP, you must first:

- configure a prefix list in the **config>router>policy-options>prefix-list** context
- configure a route policy statement in the **config>router>policy-options>policy-statement** context and apply the prefix list
  - in the **config>router>policy-options>policy-statement>entry>to** context, specify the host source addresses for which ARP requests can or cannot be forwarded to non-local networks, depending on the specified action
  - in the **config>router>policy-options>policy-statement>entry>from** context, specify the network prefixes that ARP requests will or will not be forwarded to, depending on the specified action if a match is found

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
   default-action {accept | next-entry |
     next-policy | reject}
   entry entry-id
      action {accept | next-entry | next-policy |
        reject}
      from
        prefix-list name [name...(up to 5 max)]
      to
        prefix-list name [name...(up to 5 max)]
```

The following example displays the proxy ARP configuration output.

```
A:ALU-B>config>router>policy-options# info
----------------------------------------------
            prefix-list "prefixlist1"
                prefix 10.2.2.0/24 exact
            exit
            policy-statement "proxyARPpolicy"
                entry 1
                    from
                         prefix-list "prefix-list1"
                    exit
                    to
                         prefix-list "prefix-list1"
                    exit
                    action accept
                    exit
                exit
                default-action reject
                exit
            exit
----------------------------------------------
```

For more information on route policies, see Route Policies.

Apply the policy statement to the proxy ARP policy in the **config>router>if>proxy-arp-policy** context.

CLI Syntax:

```
config>router
   interface ip-int-name
      proxy-arp-policy policy-name [policy-name...(up to
        5 max)]
```

The following example displays the router interface proxy ARP configuration.

```
A:ALU-41>config>router>if# info
----------------------------------------------
...
             address 192.168.0.255/16
             remote-proxy-arp
             proxy-arp-policy "proxyARPpolicy"
----------------------------------------------
```

3.9.13 Configuring a Security Zone

To configure NAT or firewall security functionality, you must:

- configure a NAT or firewall security profile and policy in the **config>security** context
  - in the **config>security>profile** context, specify the timeouts for the TCP/UDP/ICMP protocols and configure logging and application assurance parameters. This step is optional. If you do not configure the profile, a default profile is assigned.
  - in the **config>security>policy** context, configure a security policy, and specify the match criteria and the action to be applied to a packet if a match is found
- configure a security zone and apply the policy ID to the zone, as shown in the CLI syntax below

CLI Syntax:

```
config>router
   abort
   begin
   commit
   zone zone-id [create]
      description description-string
      interface ip-int-name [create]
      name zone-name
      nat
         pool pool-id [create]
            description description-string
            direction {zone-outbound | zone-inbound | both}
            entry entry-id [create]
               ip-address ip-address [to ip-address]
                  interface ip-int-name
               port port [to port] interface ip-int-name
            name pool-name
      policy policy-id | policy-name
      shutdown
```

The following example displays a NAT zone configuration output.

```
A:ALU-B>config>router# info
----------------------------------------------
        configure
            router
                zone 1 create
                begin
                    name "GRT zone"
                    description "uplink zone to public"
                    nat
                        pool 1 create
```

```
                            description "pool 1"
                            direction zone-outbound
                            entry 1 create
                                ip-addr 198.51.100.1
                                port 5000 to 6000
                            exit
                        exit
                    exit
                    policy 1
                    commit
                exit
                no-shutdown
-----------------------------------------------
A:ALU-B>config>router#
```

3.9.14 Configuring Security Logging

The 7705 SAR supports rule-based logging (that is, logging for each entry of a security policy) and zone-based logging.

Logging is suppressed by default. To enable either rule-based logging or zone-based logging, logging must be configured as part of the security policy configuration.

3.9.14.1 Rule-Based Security Logging

If a packet does not match any of the rules in a security policy, the packet is dropped from a security session because the default security policy action is to reject non-matching packets. With rule-based logging, in order to see that event in the event log, the policy must be configured with a rule to log rejected, non-matching packets to the **log-id**, and this rule must be configured as the last entry in the policy.

Note: If the **policy>entry>logging to log-id** command is enabled, the **zone>log** command cannot be enabled because a **log-id** cannot be configured at both the policy and zone levels.

Use the following CLI syntax to configure rule-based security logging:

CLI Syntax:

```
config>security
   logging
      profile {profile-id | profile-name} [create]
         description description-string
         event-control event-type [event event] {suppress
            | throttle | off}
         name name
```

```
      exit
      log-id {log-id | log-name} [create]
        description description-string
        destination {memory [size] | syslog syslog-id}
        name name
        profile {logging-profile-id | logging- profile-
          name}
        no shutdown
      exit
    exit
    begin
    policy {profile-id | profile-name} [create]
      name profile-name
      description description-string
      application
        assurance
          dns
            [no] reply-only
          icmp
            [no] limit-type3
            request limit packets
            no request limit
          ip
            options {permit ip-option-mask | permit-any}
            options ip-option-name [ip-option-name]
          tcp
            [no] strict
          exit
        exit
      exit
      timeouts
      exit
    exit
    policy {policy-id | policy-name} [create]
      description description-string
      entry entry-id
        match [protocol {protocol-id | name}]
          direction {zone-outbound | zone-inbound | both}
          src-ip ip-address to ip-address
        action reject
        logging to log-id {log-id | log-name}
        exit
      exit
```

The following example displays a rule-based logging configuration output.

```
*A:7705:Dut-C>config>security# info
----------------------------------------------
    logging
        profile 2 create
```

```
            event-control "policy" event "1" throttle
            event-control "policy" event "2" throttle
        exit
        profile 100 create
            event-control "policy" event "1" throttle
            event-control "policy" event "2" throttle
        exit
        log-id 10 create
            name "SecurityLog10"
            description "Security Log ID 10"
            destination memory 1024
            profile "100"
            no shutdown
        exit
        log-id 20 create
            name "SecurityLog20"
            description "Security Log ID 20"
            destination memory 1024
            no shutdown
        exit
        log-id 30 create
            name "SecurityLog30"
            description "Security Log ID 30"
            destination memory 1024
            no shutdown
        exit
        log-id 40 create
            name "SecurityLog40"
            description "Security Log ID 40"
            destination memory 1024
            profile "100"
            no shutdown
        exit
        log-id 50 create
            name "SecurityLog50"
            description "Security Log ID 50"
            destination memory 1024
            no shutdown
        exit
        log-id 100 create
            name "SecurityLog100"
            description "Security Log ID 100"
            destination memory 1024
            no shutdown
        exit
    exit
    begin
    profile 10 create
        name "StrictTCP"
        description "Strict TCP Enabled"
        application
            assurance
                ip
                exit
                icmp
                exit
                tcp
                    strict
                exit
```

```
            dns
            exit
        exit
    exit
    timeouts
    exit
exit
profile 20 create
    name "DNS"
    description "DNS_Reply_Strict"
    application
        assurance
            ip
            exit
            icmp
            exit
            tcp
            exit
            dns
            exit
        exit
    exit
    timeouts
    exit
exit
profile 30 create
    name "ICMP"
    description "ICMP Type3 Response Limit"
    application
        assurance
            ip
            exit
            icmp
            exit
            tcp
            exit
            dns
            exit
        exit
    exit
    timeouts
    exit
exit
policy 10 create
    description "Strict TCP"
    entry 10 create
        description "Entry 10"
        match protocol tcp
            direction zone-outbound
            src-ip 10.1.1.2
        exit
        limit
        exit
        action forward
        profile "StrictTCP"
        logging to log-id "SecurityLog10"
    exit
    entry 20 create
        description "TCP"
```

```
                match protocol tcp
                    direction zone-outbound
                exit
                limit
                exit
                action forward
                logging to log-id "SecurityLog20"
            exit
            entry 30 create
                description "UDP and DNS"
                match protocol udp
                    direction zone-outbound
                exit
                limit
                exit
                action forward
                profile "DNS"
                logging to log-id "SecurityLog30"
            exit
            entry 40 create
                description "ICMP"
                match protocol icmp
                    direction zone-outbound
                exit
                limit
                exit
                action forward
                profile "ICMP"
                logging to log-id "SecurityLog40"
            exit
            entry 50 create
                description "SCTP Drop Rule"
                match protocol sctp
                    direction zone-outbound
                exit
                limit
                exit
                action drop
                logging to log-id "SecurityLog50"
            exit
            entry 255 create
                description "Non Supported Protocol Rule"
                match
                exit
                limit
                exit
                logging to log-id "SecurityLog100"
            exit
        exit
    ------------------------------------------------
    *A:7705:Dut-C>config>security#
```

The following example displays the error that occurs when there is an attempt to configure a **log-id** at both the policy level and the zone level.

```
*A:7705:Dut-C>config>service>vprn# info
----------------------------------------------
            route-distinguisher 65000:1
            vrf-target target:1:1
            interface "vprn-1-10.1.1.1" create
                address 192.168.0.0/16
                ip-mtu 1500
                spoke-sdp 1:10 create
                    no shutdown
                exit
            exit
            interface "vprn-1-10.1.1.1" create
                address 192.168.0.1/16
                ip-mtu 1500
                spoke-sdp 3:20 create
                    no shutdown
                exit
            exit
            zone 10 create
                description "Zone 10: "
                interface "vprn-1-10.1.1.1"
                exit
                nat
                exit
                policy "10"
                inbound
                    limit
                    exit
                exit
                outbound
                    limit
                    exit
                exit
                commit
            exit
            no shutdown
----------------------------------------------
*A:7705:Dut-C>config>service>vprn#   zone 10 log 100
MINOR: FIREWALL #1086 Policy level rule logging enabled. - Can not configure
logids at both policy and zone levels
```

3.9.14.2 Zone-Based Security Logging

Zone-based logging is enabled when the **config>security>policy>entry>logging to zone** command is configured as part of the security policy configuration. Zone-based logging can be configured after the policy has been created, but this requires the **begin** and **commit** actions, which cause existing security sessions to be cleared.

Use the following CLI syntax to configure zone-based security logging:

CLI Syntax:

```
config>security
   logging
      profile {profile-id | profile-name} [create]
         description description-string
         event-control event-type [event event] {suppress
            | throttle | off}
         name name
      log-id {log-id | log-name} [create]
         description description-string
         destination {memory [size] | syslog syslog-id}
         name name
         profile {logging-profile-id | logging- profile-
            name}
         no shutdown
         exit
      exit
   profile {profile-id | profile-name} [create]
      description description-string
      name name
      application
         assurance
            dns
               reply-only
            tcp
               strict
               exit
            exit
         exit
      exit
   policy {policy-id | policy-name} [create]
      description description-string
      entry entry-id
         match [protocol {protocol-id | name}]
            direction {zone-outbound | zone-inbound | both}
            src-ip ip-address to ip-address
         action {drop | forward | nat | reject}
         logging to zone
```

The following example displays a zone-based logging configuration output.

```
*A:7705:Dut-C>config>security# info
----------------------------------------------
    logging
        profile 10 create
            event-control "packet" event "10" suppress
        exit
        log-id 10 create
            name "SecurityLog10"
```

```
            description "Security Log ID 10"
            destination memory 1024
            profile "10"
            no shutdown
        exit
        log-id 11 create
            destination memory 1024
            no shutdown
        exit
    exit
    profile 100 create
        name "StrictTCP"
        description "Strict TCP Enabled"
        application
            assurance
                ip
                exit
                icmp
                exit
                tcp
                    strict
                exit
                dns
                exit
            exit
        exit
        timeouts
        exit
    exit
    profile 101 create
        name "SessTimeout"
        description "timout"
        application
            assurance
                ip
                exit
                icmp
                exit
                tcp
                    strict
                exit
                dns
                exit
            exit
        exit
        timeouts
            other-sessions idle sec 40
        exit
    exit
    policy 10 create
        name "Mixed bag"
        description "Ingress Uni-directional"
        entry 1 create
            description "unknown"
            match protocol 48
                direction zone-outbound
            exit
            limit
            exit
```

```
        action forward
        logging to zone
    exit
    entry 2 create
        description "UDPLite"
        match protocol 136
            direction zone-outbound
        exit
        limit
        exit
        action forward
        logging to zone
    exit
    entry 3 create
        description "TCP"
        match protocol tcp
            direction zone-outbound
            src-port range 1024 15000
        exit
        limit
        exit
        action forward
        logging to zone
    exit
    entry 4 create
        description "Strict TCP"
        match protocol tcp
            direction zone-outbound
            src-port lt 1024
        exit
        limit
        exit
        action forward
        profile "StrictTCP"
        logging to zone
    exit
    entry 5 create
        description "GRE"
        match protocol gre
            direction zone-outbound
        exit
        limit
        exit
        action forward
        logging to zone
    exit
    entry 6 create
        description "UDP bad"
        match protocol udp
            direction zone-outbound
            src-port lt 1024
        exit
        limit
        exit
        logging to zone
    exit
    entry 7 create
        description "UDP good"
        match protocol udp
```

```
                direction zone-outbound
                src-port gt 1024
            exit
            limit
            exit
            action forward
            logging to zone
        exit
        entry 8 create
            description "UDP bad"
            match protocol udp
                direction zone-outbound
                src-port eq 1024
            exit
            limit
            exit
            action drop
            logging to zone
        exit
        entry 9 create
            description "IPv6 Encap"
            match protocol ipv6
                direction zone-outbound
            exit
            limit
            exit
            action forward
            logging to zone
        exit
    exit
    commit
-----------------------------------------------
*A:7705:Dut-C>config>security#
```

The following example displays a zone-based logging configuration output for a VPRN service.

```
*A:7705:Dut-C>config>service>vprn# info
----------------------------------------------
            route-distinguisher 65000:1
            vrf-target target:1:1
            interface "vprn-1-10.1.1.1" create
                address 192.168.0.0/16
                ip-mtu 1500
                spoke-sdp 1:10 create
                    no shutdown
                exit
            exit
            interface "vprn-1-10.1.1.2" create
                address 192.168.0.1/16
                ip-mtu 1500
                spoke-sdp 3:20 create
                    no shutdown
                exit
            exit
            zone 10 create
                description "Zone 10: "
                interface "vprn-1-10.1.1.1"
```

```
                    exit
                    nat
                    exit
                    policy "Mixed bag"
                    inbound
                        limit
                        exit
                    exit
                    outbound
                        limit
                        exit
                    exit
                    log "SecurityLog10"
                    commit
                exit
                no shutdown
----------------------------------------------
```

3.9.15 Applying an Application Group and a Host Group to a Security Policy

Use the following CLI syntax to apply an application group or a host group to a security policy:

CLI Syntax:

```
config>security
  app-group {id | name} [create]
    name name
    description description
    entry entry-id [create]
      match [protocol {protocol-id | protocol-name}]
    exit
  exit
  host-group {id | name} [create]
    name name
    description description
    host ip-address [to ip-address]
    exit
  exit
  policy {policy-id | policy-name} [create]
    description description-string
    entry entry-id
      description description-string
      match [local] [protocol {protocol-id | name}]
      match [local] [protocol {tcp| udp | *}]
      match [app-group {group-id| name}]
        direction {zone-outbound | zone-inbound | both}
        src-ip host-group {group-id | name}
```

```
                    action {forward | reject |drop | nat}
                    profile {profile-id | profile-name}
                    logging to log-id {log-id | log-name}| suppressed
                       | to zone}
                    exit
                exit
```

The following output is an example of applying an application group and a host group to a security policy:

```
*A:7705:Dut-A>config>security>policy# info
----------------------------------------------
    name "Inbound Policy"
    description "Common egress policy"
    entry 1 create
        description "match TCP and IP"
        match app-group "Telnet"
            direction zone-inbound
            src-ip host-group "Private Hosts"
        exit
        limit
        exit
        action nat
        profile "nonDefault1"
        logging to zone
    exit
    entry 2 create
        description "match UDP and port"
        match app-group "SNMP"
            direction zone-inbound
        exit
        limit
        exit
        action nat
        profile "nonDefault1"
        logging to zone
    exit
    entry 3 create
        description "match ISAKMP"
        match protocol udp
            direction zone-inbound
            src-ip host-group "Private Hosts"
            dst-port eq 500
        exit
        limit
        exit
        action nat
        profile "nonDefault1"
        logging to zone
    exit
----------------------------------------------
*A:7705:Dut-A>config>security>policy#
```

3.9.16 Configuring an IP Reassembly Profile

The IP reassembly function is used to reassemble IP fragments received at a GRE tunnel egress. A reassembly profile is used to specify the amount of buffer space allocated for the IP reassembly function and to configure a reassembly timeout.

Use the following CLI syntax to create and configure an IP reassembly profile.

CLI Syntax:

```
config>router
  reassembly
    reassembly-profile profile-id create
      cbs size-in-kbytes
      description description-string
      epd-threshold percent
      fc fc-name create
        cbs-override size-in-kbytes
        mbs-override size [bytes | kilobytes]
        wait-override milli-seconds
      mbs size [bytes | kilobytes]
      wait milli-seconds
```

Example:

```
A:ALU-A>config>router# reassembly
A:ALU-A>config>router>reassembly# reassembly-profile 1
 create
A:ALU-A>config>router>reassembly>reassembly-profile#
 cbs 50
A:ALU-A>config>router>reassembly>reassembly-profile#
 description RP1
A:ALU-A>config>router>reassembly>reassembly-profile#
 epd-threshold 75
A:ALU-A>config>router>reassembly>reassembly-profile# fc
 nc create
A:ALU-A>config>router>reassembly>reassembly-profile>fc#
 cbs-override 40
A:ALU-A>config>router>reassembly>reassembly-profile>fc#
 mbs-override 600 kilobytes
A:ALU-A>config>router>reassembly>reassembly-profile>fc#
 wait-override 1500
A:ALU-A>config>router>reassembly>reassembly-profile>fc#
 exit
A:ALU-A>config>router>reassembly>reassembly-profile#
 mbs 650 kilobytes
A:ALU-A>config>router>reassembly>reassembly-profile#
 wait 2500
```

The following output is an example of a configured IP reassembly profile.

```
*A:ALU-A>config>router>reassembly# info
----------------------------------------------
 reassembly-profile 1 create
                description "RP1"
                cbs 50
                mbs 650 kilobytes
                wait 2500
                epd-threshold 75
                fc "nc" create
                    wait-override 1500
                    cbs-override 40
                    mbs-override 600 kilobytes
                exit
            exit
----------------------------------------------
*A:ALU-A>config>router>reassembly#
```

Use the following CLI syntax to assign an IP reassembly profile to an interface.

CLI Syntax: `config>router# interface` *`ip-int-name`*
`reassembly-profile` *`profile-id`*

Example:
```
A:ALU-A>config>router# interface SDP1
A:ALU-A>config>router>if# reassembly-profile 1
```

The following output is an example of an interface with an assigned IP reassembly profile.

```
*A:ALU-A>config>router>if# info
----------------------------------------------
 reassembly-profile 1
 no shutdown
----------------------------------------------
```

3.10 Service Management Tasks

This section discusses the following service management tasks:

- Changing the System Name
- Modifying Interface Parameters
- Deleting a Logical IP Interface

3.10.1 Changing the System Name

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

Use the following CLI syntax to change the system name:

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

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

The following example displays the system name change.

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

3.10.2 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 192.168.0.0/16
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 192.168.0.10/16
        exit
        interface "to-sr1"
            address 192.168.0.0/16
            port 1/1/2
        exit
        router-id 192.168.0.1

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

3.10.3 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#
```

3.11 IP Router Command Reference

3.11.1 Command Hierarchies

- Configuration Commands
  - Router Commands
  - Local DHCP and DHCPv6 Server Commands
  - Router BFD Commands
  - Seamless BFD Reflector Commands
  - Router Interface Commands
  - Router Interface IPv6 Commands
  - Router Advertisement Commands
  - Router Security Zone Configuration Commands
  - Static One-to-One NAT Configuration Commands
  - TWAMP Light Commands
- Show Commands
- Clear Commands
- Debug Commands

3.11.1.1 Configuration Commands

3.11.1.1.1 Router Commands

config
- **router** [*router-name*]
  - **aggregate** *ip-prefix/ip-prefix-length* [**summary-only**] [**as-set**] [**aggregator** *as-number:ip-address*] [**description** *description-string*]
  - **no aggregate** *ip-prefix/ip-prefix-length*
  - [**no**] **allow-icmp-redirect**
  - **autonomous-system** *as-number*
  - **no autonomous-system**
  - [**no**] **bgp**
  - **dhcp**
  - **ecmp** *max-ecmp-routes*
  - **no ecmp**
  - [**no**] **entropy-label**
  - **if-attribute**
    - **admin-group** *group-name* **value** *group-value*
    - **no admin-group** *group-name*
    - **srlg-group** *group-name* **value** *group-value*
    - **no srlg-group** *group-name*
  - [**no**] **igmp**
  - [**no**] **ip-fast-reroute**
  - **ipv6**
    - [**no**] **reachable-time** *seconds*
    - [**no**] **stale-time** *seconds*
  - [**no**] **interface** *ip-int-name*
  - [**no**] **isis**
  - [**no**] **ldp**
  - [**no**] **mld**
  - [**no**] **mpls**
  - **mpls-labels**
    - **sr-labels start** *start-value* **end** *end-value*
    - **no sr-labels**
    - **static-label-range** *static-range*
    - **no static-label-range**
  - [**no**] **ospf**
  - [**no**] **pim**
  - [**no**] **policy-options**
  - **reassembly**
    - **reassembly-profile** *profile-id* [**create**]
    - **no reassembly-profile** *profile-id*
      - **cbs** *size-in-kbytes*
      - **description** *description-string*
      - **epd-threshold** *percent*
      - **fc** *fc-name* [**create**]
      - **no fc** *fc-name*
        - **cbs-override** *size-in-kbytes*
        - **no cbs-override**
        - **mbs-override** *size* [**bytes** | **kilobytes**]

```
            — no mbs-override
            — wait-override milli-seconds
            — no wait-override
         — mbs size [bytes | kilobytes]
         — wait milli-seconds
   — [no] rip
   — route-next-hop-policy
      — abort
      — begin
      — commit
      — [no] template template-name
         — description description-string
         — [no] exclude-group ip-admin-group-name
         — include-group ip-admin-group-name [pref preference]
         — no include-group ip-admin-group-name
         — nh-type {ip | tunnel}
         — no nh-type
         — protection-type {link | node}
         — no protection-type
         — [no] srlg-enable
   — router-id ip-address
   — no router-id
   — rsvp
   — sgt-qos
   — service-prefix {ip-prefix/prefix-length | ip-prefix netmask} [exclusive]
   — no service-prefix {ip-prefix/prefix-length | ip-prefix netmask}
   — [no] static-route-entry {ip-prefix/prefix-length} [mcast]
      — [no] black-hole
         — [no] description description-string
         — [no] metric metric
         — [no] preference preference
         — [no] shutdown
         — [no] tag tag
      — [no] indirect ip-address
         — [no] description description-string
         — [no] metric metric
         — [no] preference preference
         — [no] shutdown
         — [no] tag tag
         — tunnel-next-hop
            — [no] disallow-igp
            — resolution {any | disabled | filter}
            — resolution-filter
               — [no] ldp
               — [no] rsvp-te
                  — [no] lsp lsp-name
               — [no] sr-isis
               — [no] sr-ospf
               — [no] sr-te
                  — [no] lsp lsp-name
      — [no] next-hop {ip-address | ip-int-name | ipv6-address}
         — [no] bfd-enable
         — [no] description description-string
         — [no] ldp-sync
```

— [no] metric *metric*
— [no] preference *preference*
— [no] shutdown
— [no] tag *tag*

3.11.1.1.2 Local DHCP and DHCPv6 Server Commands

```
config
    — router
        — dhcp
            — local-dhcp-server server-name [create]
            — no local-dhcp-server server-name
                — description description-string
                — no description
                — [no] force-renews
                — pool pool-name [create]
                — no pool pool-name
                    — description description-string
                    — no description
                    — max-lease-time [days days] [hrs hours] [min minutes] [sec seconds]
                    — no max-lease-time
                    — min-lease-time [days days] [hrs hours] [min minutes] [sec seconds]
                    — no min-lease-time
                    — minimum-free minimum-free [percent] [event-when-depleted]
                    — no minimum-free
                    — offer-time [min minutes] [sec seconds]
                    — no offer-time
                    — options
                        — custom-option option-number address ip-address [ip-address...(up to 4
                            max)]
                        — custom-option option-number hex hex-string
                        — custom-option option-number string ascii-string
                        — no custom-option option-number
                        — dns-server ip-address [ip-address...(up to 4 max)]
                        — no dns-server
                        — domain-name domain-name
                        — no domain-name
                        — lease-rebind-time [days days] [hrs hours] [min minutes] [sec seconds]
                        — no lease-rebind-time
                        — lease-renew-time [days days] [hrs hours] [min minutes] [sec seconds]
                        — no lease-renew-time
                        — lease-time [days days] [hrs hours] [min minutes] [sec seconds]
                        — no lease-time
                        — netbios-name-server ip-address [ip-address...(up to 4 max)]
                        — no netbios-name-server
                        — netbios-node-type {B | P | M | H}
                        — no netbios-node-type
                    — subnet {ip-address mask | ip-address netmask} [create]
                    — no subnet {ip-address mask | ip-address netmask}
                        — [no] address-range start-ip-address end-ip-address
                        — [no] exclude-addresses start-ip-address [end-ip-address]
```

- **maximum-declined** *maximum-declined*
- **no maximum-declined**
- **minimum-free** *minimum-free* [**percent**] [**event-when-depleted**]
- **no minimum-free**
- **options**
- **custom-option** *option-number* **address** *ip-address* [*ip-address*...(up to 4 max)]
- **custom-option** *option-number* **hex** *hex-string*
- **custom-option** *option-number* **string** *ascii-string*
- **no custom-option** *option-number*
- **default-router** *ip-address* [*ip-address*...(up to 4 max)]
- **no default-router**
- **subnet-mask** *ip-address*
- **no subnet-mask**
- [**no**] **shutdown**
- [**no**] **use-gi-address**
- [**no**] **use-pool-from-client**
- **dhcp6**
- **local-dhcp-server** *server-name* [**create**]
- **no local-dhcp-server** *server-name*
- **description** *description-string*
- **no description**
- [**no**] **ignore-rapid-commit**
- **lease-hold-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
- **no lease-hold-time**
- **pool** *pool-name* [**create**]
- **no pool** *pool-name*
- **description** *description-string*
- **no description**
- **options**
- **custom-option** *option-number* **address** *ipv6-address* [*ipv6-address*...(up to 4 max)]
- **custom-option** *option-number* **domain** *domain-string*
- **custom-option** *option-number* **hex** *hex-string*
- **custom-option** *option-number* **string** *ascii-string*
- **no custom-option** *option-number*
- **dns-server** *ipv6-address* [*ipv6-address*...(up to 4 max)]
- **no dns-server**
- **domain-name** *domain-name*
- **no domain-name**
- **prefix** *ipv6-address/prefix-length* [**pd**] [**wan-host**] [**create**]
- **no prefix** *ipv6-address/prefix-length*
- **options**
- **custom-option** *option-number* **address** *ipv6-address* [*ipv6-address*...(up to 4 max)]
- **custom-option** *option-number* **domain** *domain-string*
- **custom-option** *option-number* **hex** *hex-string*
- **custom-option** *option-number* **string** *ascii-string*
- **no custom-option** *option-number*
- **dns-server** *ipv6-address* [*ipv6-address*...(up to 4 max)]
- **no dns-server**
- **domain-name** *domain-name*
- **no domain-name**
- **preferred-lifetime** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]

```
            — no preferred-lifetime
            — rebind-timer [days days] [hrs hours] [min minutes] [sec seconds]
            — no rebind-timer
            — renew-timer [days days] [hrs hours] [min minutes] [sec seconds]
            — no renew-timer
            — valid-lifetime [days days] [hrs hours] [min minutes] [sec seconds]
            — no valid-lifetime
         — server-id duid-en hex hex-string
         — server-id duid-en string ascii-string
         — server-id duid-ll
         — no server-id
         — [no] shutdown
         — use-link-address [scope scope]
         — no use-link-address
         — [no] use-pool-from-client
         — user-ident user-ident
         — no user-ident
```

3.11.1.1.3 Router BFD Commands

```
config
   — router [router-name]
      — bfd
         — bfd-template name
         — no bfd-template
            — multiplier multiplier
            — no multiplier
            — receive-interval receive-interval
            — no receive-interval
            — transmit-interval transmit-interval
            — no transmit-interval
            — type np
            — no type
         — seamless-bfd
            — [no] peer {ip-address | ipv6-address}
               — discriminator discriminator
               — no discriminator
```

3.11.1.1.4 Seamless BFD Reflector Commands

```
config
    — bfd
        — seamless-bfd
            — reflector reflector-name
            — no reflector
                — description description-string
                — no description
                — discriminator discriminator
                — no discriminator
                — local-state {admin-down | up}
                — no local-state
                — [no] shutdown
```

3.11.1.1.5 Router Interface Commands

```
config
    — router [router-name]
        — [no] interface ip-int-name
            — address {ip-address/mask | ip-address netmask | dhcp} [client-identifier [ascii-value
                | interface-name]] [vendor-class-id vendor-class-id]
            — no address
            — [no] allow-directed-broadcasts
            — arp-retry-timer ms-timer
            — no arp-retry-timer
            — arp-timeout seconds
            — no arp-timeout
            — bfd transmit-interval [receive receive-interval] [multiplier multiplier] [type np]
            — no bfd
            — cflowd-parameters
                — sampling {unicast | multicast} type {interface} [direction {ingress-only |
                    egress-only | both}]
                — no sampling {unicast | multicast}
            — description description-string
            — no description
            — dhcp
                — description description-string
                — no description
                — gi-address ip-address [src-ip-addr]
                — no gi-address
                — [no] option
                    — action {replace | drop | keep}
                    — no action
                    — circuit-id [ascii-tuple | port-id | if-name]
                    — no circuit-id
                    — [no] copy-82
                    — remote-id [mac | string string]
                    — no remote-id
                — server server1 [server2...(up to 8 max)]
                — no server
```

- [no] shutdown
- egress
  - agg-rate-limit *agg-rate* [cir *cir-rate*]
  - no agg-rate-limit
  - filter ip *ip-filter-id*
  - filter ipv6 *ipv6-filter-id*
  - no filter [ip *ip-filter-id* | ipv6 *ipv6-filter-id*]
  - queue-policy *name*
  - no queue-policy
- eth-cfm
  - mep *mep-id* domain *md-index* association *ma-index*
  - no mep *mep-id* domain *md-index* association *ma-index*
    - [no] ccm-enable
    - ccm-ltm-priority *priority*
    - no ccm-ltm-priority
    - ccm-tlv-ignore [port-status] [interface-status]
    - no ccm-tlv-ignore
    - description *description-string*
    - no description
    - [no] dual-ended-loss-test-enable
      - alarm-threshold *percentage*
      - no alarm-threshold
      - alarm-clear-threshold *percentage*
      - no alarm-clear-threshold
    - [no] eth-test-enable
      - bit-error-threshold *bit-errors*
      - [no] test-pattern {all-zeros | all-ones} [crc-enable]
    - low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
    - one-way-delay-threshold *seconds*
    - [no] shutdown
- [no] group-encryption
  - encryption-keygroup *keygroup-id* direction {inbound | outbound}
  - no encryption-keygroup direction {inbound | outbound}
  - ip-exception *filter-id* direction {inbound | outbound}
  - no ip-exception direction {inbound | outbound}
- icmp
  - [no] mask-reply
  - ttl-expired [*number seconds*]
  - no ttl-expired
  - unreachables [*number seconds*]
  - no unreachables
- if-attribute
  - [no] admin-group *group-name* [*group-name*...(up to 5 max)]
  - [no] srlg-group *group-name* [*group-name*...(up to 5 max)]
- ingress
  - filter ip *ip-filter-id*
  - filter ipv6 *ipv6-filter-id*
  - no filter [ip *ip-filter-id* | ipv6 *ipv6-filter-id*]
- ldp-sync-timer *seconds*
- no ldp-sync-timer
- load-balancing
  - l4-load-balancing *hashing-algorithm*
  - no l4-load-balancing

```
            — lsr-load-balancing hashing-algorithm[bottom-of-stack hashing-treatment] [use-
                ingress-port]
            — no lsr-load-balancing
            — [no] spi-load-balancing
            — [no] teid-load-balancing
        — [no] local-dhcp-server local-server-name
        — [no] local-proxy-arp
        — [no] loopback
        — mac ieee-address
        — no mac
        — [no] multicast-translation
        — [no] ntp-broadcast
        — port port-name
        — no port
        — proxy-arp-policy policy-name [policy-name...(up to 5 max)]
        — no proxy-arp-policy
        — qos network-policy-id
        — no qos
        — [no] reassembly-profile profile
        — [no] remote-proxy-arp
        — [no] shutdown
        — static-arp ip-addr ieee-mac-addr
        — no static-arp ip-addr
        — static-arp ieee-mac-addr unnumbered
        — no static-arp unnumbered
        — tcp-mss value
        — no tcp-mss
        — unnumbered [ip-int-name | ip-address] [dhcp] [client-identifier ascii-value |
            interface-name] [vendor-class-id vendor-class-id]
        — no unnumbered
```

3.11.1.1.6 Router Interface IPv6 Commands

```
config
    — router [router-name]
        — [no] interface ip-int-name
            — [no] ipv6
                — address ipv6-address/prefix-length [eui-64] [preferred]
                — no address ipv6-address/prefix-length
                — bfd transmit-interval [receive receive-interval] [multiplier multiplier] [type np]
                — no bfd
                — icmp6
                    — packet-too-big [number seconds]
                    — no packet-too-big
                    — param-problem [number seconds]
                    — no param-problem
                    — time-exceeded [number seconds]
                    — no time-exceeded
                    — unreachables [number seconds]
                    — no unreachables
                — [no] local-dhcp-server local-server-name
```

- **link-local-address** *ipv6-address* [**preferred**]
- **no link-local-address**
- **neighbor** *ipv6-address mac-address*
- **no neighbor** *ipv6-address*
- **reachable-time** *seconds*
- **no reachable-time**
- **stale-time** *seconds*
- **no stale-time**
- **tcp-mss** *value*
- **no tcp-mss**

3.11.1.1.7 Router Advertisement Commands

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

3.11.1.1.8 Router Security Zone Configuration Commands

```
config
    — router
        — zone {zone-id | zone-name} [create]
        — no zone {zone-id | zone-name}
            — abort
            — begin
            — commit
            — description description-string
            — no description
            — inbound
                — limit
                    — concurrent-sessions {tcp |udp | icmp | other} sessions
                    — no concurrent-sessions {tcp |udp | icmp | other}
            — [no] interface interface-name
                — [no] shutdown
            — log {log-id | name}
            — no log
            — name zone-name
            — no name
            — nat
                — pool pool-id [create]
                — no pool pool-id
                    — description description-string
                    — no description
                    — direction {zone-outbound | zone-inbound | both}
                    — no direction
                    — entry entry-id [create]
                    — no entry entry-id
                        — ip-address ip-address [to ip-address] interface ip-int-name
                        — no ip-address
                        — port port [to port]
                        — no port
                    — name pool-name
                    — no name
            — outbound
                — limit
                    — concurrent-sessions {tcp |udp | icmp | other} sessions
                    — no concurrent-sessions {tcp |udp | icmp | other}
            — policy {policy-id | policy-name}
            — no policy
            — [no] shutdown
```

3.11.1.1.9 Static One-to-One NAT Configuration Commands

```
config
    — router [router-name]
        — [no] interface ip-int-name
            — [no] static-nat-inside

config
    — router
        — [no] static-nat
            — [no] drop-packets-without-nat-entry
            — inside
                — map start ip-address end ip-address to ip-address
                — no map start ip-address end ip-address
                    — [no] shutdown
```

3.11.1.1.10 TWAMP Light Commands

```
config
    — router
        — twamp-light
            — [no] reflector
                — description description-string
                — [no] prefix ip-prefix/prefix-length [create]
                    — description description-string
                — udp-port number
                — no udp-port
                — [no] shutdown
```

3.11.1.2 Show Commands

```
show
    — router router-instance
    — router service-name service-name
        — arp [ip-int-name | ip-address/[mask] | mac ieee-mac-address | summary] [arp-type]
        — authentication
            — statistics
            — statistics interface [ip-int-name | ip-address]
            — statistics policy name
        — bfd
            — interface
            — session [src ip-address [dst ip-address] | [detail]]
        — bgp
        — dhcp
            — local-dhcp-server server-name
                — associations
                — declined-addresses ip-address[/mask] [detail]
                — declined-addresses pool pool-name
```

- **free-addresses** *ip-address*[*/mask*]
- **free-addresses summary** [**subnet** *ip-address*[*/mask*]]
- **free-addresses pool** *pool-name*
- **leases** [**detail**]
- **leases** *ip-address*[*/mask*] **address-from-user-db** [**detail**]
- **leases** *ip-address*[*/mask*] [**detail**] [*state*]
- **leases** *ip-address*[*/mask*] **dhcp-host** *dhcp-host-name* [**detail**]
- **pool-ext-stats** [*pool-name*]
- **server-stats**
- **subnet-ext-stats** *ip-address*[*/mask*]
- **subnet-ext-stats pool** *pool-name*
- **subnet-stats** *ip-address*[*/mask*]
- **subnet-stats pool** *pool-name*
- **summary**

- **servers** [**all**]
- **statistics** [**interface** *ip-int-name* | *ip-address*]
- **summary**

- **dhcp6**
  - **local-dhcp-server** *server-name*
    - **associations**
    - **leases** [*ipv6-address*/*prefix-length*] [*type*] [*state*] [**detail**]
    - **pool-ext-stats** [*pool-name*]
    - **pool-stats** [*pool-name*]
    - **prefix-ext-stats** *ipv6-address*/*prefix-length*
    - **prefix-ext-stats pool** *pool-name*
    - **prefix-stats** *ipv6-address*/*prefix-length*
    - **prefix-stats pool** *pool-name*
    - **server-stats**
    - **summary**
  - **servers** [**all**]
  - **statistics**
  - **summary**
- **ecmp**
- **fib** *slot-number* [*family*] [*ip-prefix/prefix-length* [**longer**]] [**secondary**]
- **fib** *slot-number* **extensive** [*ip-prefix/prefix-length*] [*family*] [**all**]
- **fib** *slot-number* [*family*] **summary**
- **fib** *slot-number* **nh-table-usage**
- **icmp**
  - **interface** *interface-name*
- **icmp6**
  - **interface** *interface-name*
- **interface** [{[*ip-address* | *ip-int-name*] [**detail**] [*family*]} | **summary** | **exclude-services**]
- **interface** {*ip-address* | *ip-int-name*} **statistics**
- **interface** {*ip-address* | *ip-int-name*} **security**
- **interface** {*ip-address* | *ip-int-name*} **tcp-mss**
- **isis**
- **ldp**
- **mpls**
- **neighbor** [*ip-address* | *ip-int-name* | **mac** *ieee-mac-address* | **summary**] [**dynamic** | **static** | **managed**]
- **ospf**
- **policy**
- **reassembly-profile** [*profile-id*] [**detail**]
- **route-next-hop-policy template**

- **route-table** [*family*] [*ip-prefix*[*/prefix-length*] [**longer** | **exact** | **protocol** *protocol-name*] [**all**]] [**next-hop-type** *type*] [**alternative**]
- **route-table** [*family*] **summary**
- **route-table** [*family*] [*ip-prefix*[*/prefix-length*]] [**longer** | **exact** | **protocol** *protocol-name*] **extensive** [**all**]
- **rsvp**
- **rtr-advertisement** [**interface** *interface-name*] [**prefix** *ipv6-prefix/prefix-length*] [**conflicts**]
- **sgt-qos**
- **static-arp** [*ip-address* | *ip-int-name* | **mac** *ieee-mac-addr*]
- **static-route** [*family*] [*ip-prefix/prefix-length* | **preference** *preference* | **next-hop** *ip-address* | **tag** *tag*] [**detail**]
- **status**
- **tunnel-table summary** [**ipv4** | **ipv6**]
- **tunnel-table** [**protocol** *protocol*] {**ipv4** | **ipv6**}
- **tunnel-table** [*ip-prefix*[*/mask*]] [**alternative**] [**ipv4** | **ipv6**] **detail**
- **tunnel-table** [*ip-prefix*[*/mask*]] [**alternative**]
- **tunnel-table** [*ip-prefix*[*/mask*]] **protocol** *protocol* [**detail**]
- **tunnel-table** [*ip-prefix*[*/mask*]] **sdp** *sdp-id*
- **twamp-light**

3.11.1.3 Clear Commands

clear
- **router** *router-instance*
- **router service-name** *service-name*
  - **arp** {**all** | *ip-addr* | **interface** {*ip-int-name* | *ip-addr*}}
  - **authentication**
    - **statistics** [**interface** {**ip-int-name** | **ip-address**}]
  - **bfd**
    - **session src-ip** *ip-address* **dst-ip** *ip-address*
    - **session all**
    - **statistics src-ip** *ip-address* **dst-ip** *ip-address*
    - **statistics all**
  - **bgp**
  - **dhcp**
    - **local-dhcp-server** *server-name*
      - **declined-addresses** *ip-address*[*/mask*]
      - **declined-addresses pool** *pool-name*
      - **leases** *ip-address*[*/mask*] [*state*]
      - **leases all** [*state*]
      - **pool-ext-stats** [*pool-name*]
      - **server-stats**
      - **subnet-ext-stats** *ip-address*[*/mask*]
      - **subnet-ext-stats pool** *pool-name*
    - **statistics** [*ip-int-name* | *ip-address*]
  - **dhcp6**
    - **local-dhcp-server** *server-name*
      - **leases** [*ipv6-address/prefix-length*] [*type*] [*state*]
      - **leases all** [*type*] [*state*]
      - **pool-ext-stats** [*pool-name*]
      - **prefix-ext-stats** *ipv6-address/prefix-length*

```
            — prefix-ext-stats pool pool-name
            — server-stats
         — statistics
      — icmp6 all
      — icmp6 global
      — icmp6 interface interface-name
      — igmp
      — interface [ip-int-name | ip-addr] [icmp]
      — interface spoke-name statistics
      — isis
      — ldp
      — mld
      — mpls
      — neighbor {all | ip-address}
      — neighbor [interface ip-int-name | ip-address]
      — ospf
      — pim
      — rip
      — router-advertisement all
      — router-advertisement [interface interface-name]
      — rsvp
```

3.11.1.4 Debug Commands

```
debug
   — security
      — capture
         — [no] custom-format
            — [no] audit-report
            — footer footer-string
            — no footer footer-string
            — header header-string
            — no header
            — [no] packet-decode
            — packet-hex-dump [delimiter ascii-character] [byte-count] [ascii-decode]
            — no packet-hex-dump
         — destination {memory | console}
         — format {decode | raw | custom}
         — from {zone-id | name}
         — no from
         — [no] match [pass | reject] [protocol protocol-id] [src-ip src-ip-address/mask] [src-
              port src-port] [dst-ip dst-ip-address/mask] [dst-port dst-port] [size packet-size]
              [tcp-handshake]
         — start [count packets]
         — stop

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
- router service-name service-name
  - [no] bgp
  - [no] igmp
  - [no] ip
    - [no] arp
    - [no] dhcp [interface ip-int-name]
    - [no] dhcp mac ieee-address
    - [no] dhcp sap sap-id
      - detail-level {low | medium | high}
      - no detail-level
      - mode {dropped-only | ingr-and-dropped | egr-ingr-and-dropped}
      - no mode
    - dhcp6 [ip-int-name]
    - no dhcp6
      - detail-level {low | medium | high}
      - no detail-level
      - mode {dropped-only | ingr-and-dropped | egr-ingr-and-dropped}
      - no mode
    - [no] icmp
    - icmp6 [ip-int-name]
    - no icmp6
    - [no] interface [ip-int-name | ip-address]
    - [no] neighbor
    - packet [ip-int-name | ip-address] [headers] [protocol-id]
    - no packet [ip-int-name | ip-address]
    - route-table [ip-prefix/prefix-length] [longer]
    - no route-table
  - [no] isis
  - [no] ldp
  - [no] local-dhcp-server server-name [lease-address ip-prefix][/prefix-length]]
  - [no] local-dhcp-server server-name [mac ieee-address]
  - [no] local-dhcp-server server-name link-local-address ipv6z-address]
    - detail-level {low | medium | high}
    - no detail-level
    - mode {dropped-only | ingr-and-dropped | egr-ingr-and-dropped}
    - no mode
  - [no] mld
  - [no] mpls
  - [no] ospf
  - [no] pim
  - [no] rip
  - [no] rsvp

Note:

- For information on MPLS, LDP, and RSVP, refer to the 7705 SAR MPLS Guide.
- For information on OSPF, IS-IS, RIP, BGP, and multicast (IGMP, MLD, and PIM), refer to the 7705 SAR Routing Protocols Guide.
- For information on configuring ETH-CFM on network interfaces, refer to the 7705 SAR OAM and Diagnostics Guide.
- For information on self-generated traffic re-marking (sgt-qos), refer to the 7705 SAR Quality of Service Guide.
- For information on policy options, see Route Policies.

3.11.2 Command Descriptions

3.11.2.1 Configuration Commands

- Generic Commands
- Router Global Commands
- Local DHCP and DHCPv6 Server Commands
- Router BFD Commands
- Seamless BFD Reflector Commands
- Router Interface Commands
- Router Interface IPv6 Commands
- Router Interface DHCP Relay Agent Commands
- Router Interface Filter Commands
- Router Interface Encryption Commands
- Router Interface ICMP and ICMPv6 Commands
- Router Advertisement Commands
- Router Security Zone Configuration Commands
- Static One-to-One NAT Router Configuration Commands
- TWAMP Light Commands

3.11.2.1.1 Generic Commands

description

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

Context config>router>interface
config>router>if>dhcp
config>router>dhcp>local-dhcp-server
config>router>dhcp>local-dhcp-server>pool
config>router>dhcp6>local-dhcp-server
config>router>dhcp6>local-dhcp-server>pool
config>router>reassembly>reassembly-profile
config>router>route-next-hop-policy>template
config>router>static-route-entry>black-hole
config>router>static-route-entry>indirect
config>router>static-route-entry>next-hop
config>router>twamp-light>reflector
config>router>twamp-light>reflector>prefix
config>router>zone
config>router>zone>nat>pool

Description This command creates a text description stored in the configuration file for a configuration context.

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

Default no description

Parameters *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 [**no**] **shutdown**

Context config>router>interface
config>router>if>dhcp
config>router>router-advertisement>interface
config>router>dhcp>local-dhcp-server
config>router>dhcp6>local-dhcp-server
config>router>static-route-entry>black-hole
config>router>static-route-entry>indirect
config>router>static-route-entry>next-hop

config>router>twamp-light>reflector
config>router>zone
config>router>zone>interface

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

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system-generated configuration files.

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

Default no shutdown

3.11.2.1.2 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.

The router name refers to the router instance (in other commands, the router instance can be either router name or service ID). The 7705 SAR has two routing domains (instances).

The base routing domain includes all in-band IP traffic; that is, any IP packet arriving at the router over any IP interface (all services, all physical ports on the adapter cards). The routing table for the base instance is populated with these IP addresses.

The management routing domain is for out-of-band management traffic; that is, the Mgmt port on the CSM is being used for management traffic. In this case, the routing table for the management routing instance is populated.

Parameters *router-name* — the router name

Values *router-name*: Base, management

Default Base

aggregate

Syntax **aggregate** *ip-prefix/ip-prefix-length* [**summary-only**] [**as-set**] [**aggregator** *as-number:ip-address*] [**description** *description-string*]
no aggregate *ip-prefix/ip-prefix-length*

Context config>router

Description This command creates an aggregate route.

Use this command to group a number of routes with common prefixes into a single entry in the routing table. This reduces the number of routes that need to be advertised by this router and reduces the number of routes in the routing tables of downstream routers.

Both the original components and the aggregated route (source protocol aggregate) are offered to the routing table manager (RTM). Subsequent policies can be configured to assign protocol-specific characteristics, such as the OSPF tag, to aggregate routes.

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

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

The following adapter cards and platforms support the full IPv6 subnet range for IPv6 static routes:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card, version 2 and version 3
- 2-port 10GigE (Ethernet) Adapter card (on the v-port)
- 10-port 1GigE/1-port 10GigE X-Adapter card
- 7705 SAR-X

For these cards and platforms, the supported route range for statically provisioned or dynamically learned routes is from /1 to /128.

For all other cards, modules, and ports (including the v-port on the 2-port 10GigE (Ethernet) module), the supported range for statically provisioned or dynamically learned routes is from /1 to /64 or is /128 (indicating a host route).

Default no aggregate

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

Values	*ipv4-prefix*	a.b.c.d (host bits must be 0)
	ipv4-prefix-length	0 to 32
Values	*ipv6-prefix*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	ipv6-prefix-length	{0 to 128} | {0 to 64 | 128}

as-set — optional parameter only applicable to BGP. Using this parameter creates an aggregate where the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Use this parameter carefully as it can increase the amount of route churn due to best path changes.

as-number:ip-address — optional parameter that specifies the BGP aggregator path attribute to the aggregate route. When configuring the aggregator, a 2-octet AS number used to form the aggregate route must be entered, followed by the IP address of the BGP system that created the aggregate route.

Values	*as-number*:	1 to 4294967295
	ip-address:	a.b.c.d

summary-only — suppresses advertisement of more specific component routes for the aggregate

To remove the **summary-only** option, enter the same aggregate command without the **summary-only** parameter.

description-string — the description for the aggregate route, up to 80 characters long

allow-icmp-redirect

Syntax [**no**] **allow-icmp-redirect**

Context config>router

Description This command allows or drops ICMP redirects received on the management interface.

autonomous-system

Syntax **autonomous-system** *as-number*
no autonomous-system

Context config>router

Description This command defines the autonomous system (AS) number for the router. The **no** form of the command removes the defined AS number from the router.

Default n/a

Parameters *as-number* — the AS number for the router

Values 1 to 4294967295

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

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

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

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

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

Default no ecmp

Parameters *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

entropy-label

Syntax [**no**] **entropy-label**

Context config>router

Description This command, when configured, inserts the entropy label (EL) and Entropy Label Indicators (ELI) into packets where at least one LSP in the stack for the far end of the LDP or the RSVP-TE or SR-TE tunnel used by an IGP or BGP shortcut has advertised entropy label capability. If the tunnel is of type RSVP-TE or SR-TE, then **entropy-label** must also be enabled under **config>router>mpls** or **config>router>mpls>lsp**.

The result of configuring the **entropy-label** command is that other traffic that is forwarded over an LDP or an RSVP-TE or SR-TE LSP for which this router is the LER and for which there is no explicit service endpoint on the router, will have EL and ELI enabled, depending on the LSP far end advertising entropy label capability. An example of such traffic includes packets arriving on a stitched LDP LSP forwarded over an RSVP-TE LSP.

Default no entropy-label

if-attribute

Syntax **if-attribute**

Context config>router

Description This command enables the context to configure interface attributes such as administrative group and SRLG.

admin-group

Syntax **admin-group** *group-name* **value** *group-value*
no admin-group *group-name*

Context config>router>if-attribute

Description This command defines an administrative group (admin group) that can be associated with an IP or MPLS interface. Admin groups are used to tag IP and MPLS interfaces that share a specific characteristic with the same identifier. For example, an admin group identifier can represent all links that connect to core routers, or all links that have a bandwidth higher than 10 Gbytes.

Admin groups must be defined before they can be assigned to an MPLS or IP interface in the **config>router>mpls>interface** or **config>router>interface**>**if-attribute** context. Up to 32 group names can be defined. The **admin-group** names must be identical across all routers in a single domain.The IGP communicates the information throughout the area.

When admin groups are associated with MPLS interfaces, the interfaces can be included or excluded in the LSP path definition by matching on the admin-group name. CSPF will compute a path that satisfies the admin-group include and exclude constraints.

When admin groups are associated with network IP interfaces, the interfaces can be included or excluded in the route next-hop selection by matching on the admin-group name in a route next-hop policy template applied to an interface or a set of prefixes.

The system will reject the creation of an admin group if it reuses the same name but with a different group value than an existing group. The system will also reject the creation of an admin group if it reuses the same group value but with a different name than an existing group.

Only the admin groups bound to an MPLS interface are advertised area-wide in TE link TLVs and sub-TLVs when the traffic-engineering option is enabled in IS-IS or OSPF.

The **no** form of this command deletes the admin group.

Default n/a

Parameters *group-name* — specifies the name of the admin group within a router instance, up to 32 characters

group-value — specifies the group value associated with this admin group. This value is unique within a router instance.

Values 0 to 31

srlg-group

Syntax **srlg-group** *group-name* **value** *group-value*
no srlg-group *group-name*

Context config>router>if-attribute

Description This command defines a Shared Risk Link Group (SRLG) that can be associated with an IP or MPLS interface. SRLG is used to tag IP or MPLS interfaces that share the same risk of failure with the same identifier. For example, an SRLG group identifier could represent all links that use separate fibers but are carried in the same fiber conduit. If the conduit is accidentally cut, all the fiber links are cut, which means that all interfaces using these fiber links will fail.

SRLGs must be defined before they can be assigned to an MPLS or IP interface in the **config>router>mpls>interface** or **config>router>interface>if-attribute** context. Up to 256 group names can be defined. SRLG names must be identical across all routers in a single domain.

When SRLGs are associated with MPLS interfaces, CSPF at an LER will exclude the SRLGs of interfaces used by the LSP primary path when calculating the route of the secondary path. CSPF at an LER or LSR will also exclude the SRLGs of the outgoing interface of the primary LSP path in the calculation of the path of the FRR backup LSP. This provides a path disjoint between the primary path and the secondary path or FRR backup path of an LSP.

When SRLGs are associated with network IP interfaces, they are evaluated in the route next-hop selection if the **srlg-enable** option is included in a route next-hop policy template applied to an interface or a set of prefixes. For example, the SRLG constraint can be enabled to select an LFA next hop for a prefix that avoids all interfaces that share the same risk of failure as the primary next hop.

The system will reject the creation of a SRLG if it reuses the same name but with a different group value than an existing group. The system will also reject the creation of an SRLG if it reuses the same group value but with a different name than an existing group.

Only the SRLGs bound to an MPLS interface are advertised area-wide in TE link TLVs and sub-TLVs when the traffic-engineering option is enabled in IS-IS or OSPF.

The **no** form of this command deletes the SRLG.

Default n/a

Parameters *group-name* — specifies the name of the SRLG within a router instance, up to 32 characters

group-value — specifies the group value associated with this SRLG; the group value is unique within a router instance

Values 0 to 4294967295

ip-fast-reroute

Syntax [**no**] **ip-fast-reroute**

Context config>router

Description This command enables IP Fast Reroute (FRR).

IP FRR protects against link or node failures in an IP network by precalculating a backup route to use when the primary next hop is not available. Both routes are populated in the RTM.

IP FRR uses a Loop-Free Alternate (LFA) backup next hop to forward in-transit IP packets as soon as the primary next-hop failure is detected and the backup is invoked. This means that a node resumes forwarding IP packets to a destination prefix without waiting for the routing convergence. Convergence times should be similar to RSVP-TE FRR, in the tens of milliseconds.

The backup LFA is enabled when either of the following events occurs:

- an OSPF or IS-IS interface goes operationally down, due to either a physical failure or a local administrative shutdown
- a BFD session to a next hop times out when BFD is enabled on the interface

IP FRR is supported on IPv4 and IPv6 OSPF and IS-IS prefixes and on VPN-IPv4 OSPF prefixes forwarded in the base router instance. IP FRR also provides an LFA backup next hop for the destination prefix of a GRE tunnel used in an SDP or in VPRN auto-bind.

Default no ip-fast-reroute

ipv6

Syntax **ipv6**

Context config>router

Description This command enables the context to configure IPv6 neighbor discovery parameters on the router.

Default n/a

reachable-time

Syntax [**no**] **reachable-time** *seconds*

Context config>router>ipv6

Description This command specifies the time that an IPv6 neighbor remains in a reachable state.

Default no reachable-time

Parameters *seconds* — the number of seconds that an IPv6 neighbor remains in a reachable state

Values 30 to 3600

Default 30

stale-time

Syntax [**no**] **stale-time** *seconds*

Context config>router>ipv6

Description This command specifies the time that an IPv6 neighbor cache entry remains in a stale state. When the specified time elapses, the system removes the neighbor cache entry.

Default no stale-time

Parameters *seconds* — the number of seconds that an IPv6 neighbor remains in a stale state

Values 60 to 65535

Default 14400

mpls-labels

Syntax **mpls-labels**

Context config>router

Description This command creates a context for the configuration of global parameters related to MPLS labels.

sr-labels

Syntax **sr-labels start** *start-value* **end** *end-value*
no sr-labels

Context config>router>mpls-labels

Description This command configures the range of the Segment Routing Global Block (SRGB). The SRGB is a label block that is used for assigning labels to segment routing prefix SIDs originated by this router. This range is derived from the system dynamic label range and, by default, is not instantiated.

The SR label is a reserved label, and when configured it cannot be used by other protocols such as RSVP-TE, LDP, or BGP to assign a label dynamically.

Default no sr-labels

Parameters *start-value* — specifies the start label value in the SRGB

Values 18432 to 131071 within dynamic label range

end-value — specifies the end label value in the SRGB

Values 18432 to 131071 within dynamic label range

static-label-range

Syntax **static-label-range** *static-range*
no static-label-range

Context config>router>mpls-labels

Description This command configures the range of MPLS static label values shared among static LSP, MPLS-TP LSP, and static service VC labels. When this range is configured, it is reserved and cannot be used by other protocols such as RSVP-TE, LDP, BGP, or segment routing to assign a label dynamically.

Default static-label-range

Parameters *static-range* — specifies the size of the static label range in number of labels. The minimum label value in the range is 32. The maximum label value is computed as {32 + *static-range*–1}.

Values 0 to 131040

Default 18400

reassembly

Syntax **reassembly**

Context config>router

Description This command enables the context to configure reassembly profiles.

Default n/a

reassembly-profile

Syntax **reassembly-profile** *profile-id* [**create**]
no reassembly-profile *profile-id*

Context config>router>reassembly

Description This command creates a reassembly profile and enables the context to configure the reassembly profile parameters. The reassembly profile contains all of the timing information used to ensure that all expected fragments of a packet are received within an expected time frame, on a per-forwarding class basis. When the reassembly profile timers expire, all fragments of the current incomplete frame are dropped and a “Fragment Reassembly Time Exceeded” ICMP error message is sent to the source node.

The **no** form of the command deletes the specified profile.

Default n/a

Parameters *profile-id* — the identification number of the reassembly profile

Values 1 to 16

create — keyword is mandatory when creating a reassembly profile

cbs

Syntax **cbs** *size-in-kbytes*

Context config>router>reassembly>reassembly-profile

Description This command configures the CBS for all reassembly queue groups of each forwarding class that does not have a configured CBS override. The reassembly queue groups are the groups of queues that are used to reassemble fragmented packets.

Default 0

Parameters *size-in-kbytes* — the number of kilobytes reserved for the queue. Entering the **default** keyword returns the CBS to the default value of 0 kbytes.

Values 0 to 131072 | default

epd-threshold

Syntax **epd-threshold** *percent*

Context config>router>reassembly>reassembly-profile

Description This command configures the early packet discard (EPD) threshold. This value is a percentage of the MBS and CBS. When the reassembly queue group reaches the configured percentage of the MBS and CBS, all fragments of packets without existing reassembly contexts are discarded. Fragments of packets whose reassembly contexts are already created will still be accepted until the MBS and CBS is reached.

Default 50

Parameters *percent* — the EPD threshold, as a percentage. Entering the **default** keyword returns the EPD threshold to the default value of 50%.

Values 1 to 100 | default

fc

Syntax **fc** *fc-name* [**create**]
no fc *fc-name*

Context config>router>reassembly>reassembly-profile

Description This command creates a forwarding class for which exclusive CBS, MBS, and wait times can be configured.

Note: When no forwarding class is specified, the CBS, MBS, and wait times configured for the reassembly profile are used.

Default n/a

Parameters *fc-name* — the case-sensitive, system-defined forwarding class for which IP reassembly profile entries will be created

Values be, l2, af, l1, h2, ef, h1, nc

create — keyword is mandatory when defining a forwarding class for the IP reassembly profile

cbs-override

Syntax **cbs-override** *size-in-kbytes*
no cbs-override

Context config>router>reassembly>reassembly-profile>fc

Description This command configures the CBS for the specified forwarding class. This value overrides the CBS value configured for the reassembly profile.

The **no** form of the command removes the CBS override for the specified forwarding class; the CBS configured for the reassembly profile is used.

Default no cbs-override

Parameters *size-in-kbytes* — the number of kilobytes reserved for the queue for the specified forwarding class only

Values 0 to 131072

mbs-override

Syntax **mbs-override** *size* [**bytes** | **kilobytes**]
no mbs-override

Context config>router>reassembly>reassembly-profile>fc

Description This command configures the MBS for the specified forwarding class in either bytes or kilobytes. The default configuration is in kilobytes. This value overrides the MBS value configured for the reassembly profile.

Note: For the 7705 SAR, 1 kbyte of buffer management space is 1000 bytes.

The MBS value is used by a reassembly queue group to prevent exhaustion of the main buffer pool while enqueuing packet fragments. If the queue group exceeds the number of buffers allowed by MBS, all buffers previously used to reassemble packets are freed up except for one. The remaining buffer remains active until all remaining fragments of the frame are received and discarded, or the wait time expires, after which the buffer is freed up.

The sum of the MBS for all queues on an adapter card or fixed platform can exceed the total amount of buffering available. Therefore, for a packet fragment arriving at a queue group that has not exceeded its MBS size, it is not guaranteed that a buffer will be available. If a buffer is not available, the packet fragment will be discarded.

Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard against queue starvation (that is, when a queue does not receive an adequate share of buffers).

The **no** form of the command removes the MBS override for the specified forwarding class; the MBS configured for the reassembly profile is used.

Default no mbs-override

Parameters *size* — the maximum number of kilobytes (default) or bytes of buffering allowed for the reassembly queue for the specified forwarding class only

Values 0 to 131072000

bytes — specifies that *size* is measured in bytes

kilobytes — specifies that *size* is measured in kilobytes

wait-override

Syntax **wait-override** *milli-seconds*
no wait-override

Context config>router>reassembly>reassembly-profile>fc

Description This command configures the wait time for the specified forwarding class. The wait time specifies the amount of time that the IP reassembly function will wait to reassemble a packet before discarding the collected fragments. This value overrides the wait time configured for the reassembly profile.

The **no** form of the command removes the wait time override for the specified forwarding class; the wait time configured for the reassembly profile is used.

Default no wait-override

Parameters *milli-seconds* — the length of the wait time override for the specified forwarding class, in milliseconds

Values 100 to 60000

mbs

Syntax **mbs** *size* [**bytes** | **kilobytes**]

Context config>router>reassembly>reassembly-profile

Description This command configures the MBS, in either bytes or kilobytes, for all queue groups of each forwarding class that does not have a configured MBS override. The default configuration is in kilobytes.

Note: For the 7705 SAR, 1 kbyte of buffer management space is 1000 bytes.

The MBS value is used by a reassembly queue group to prevent exhaustion of the main buffer pool while enqueuing packet fragments. If the queue group exceeds the number of buffers allowed by MBS, all buffers previously used to reassemble packets are freed up except for one. The remaining buffer remains active until all remaining fragments of the frame are received and discarded, or the wait time expires, after which the buffer is freed up.

The sum of the MBS for all queues on an adapter card or fixed platform can exceed the total amount of buffering available. Therefore, for a packet fragment arriving at a queue group that has not exceeded its MBS size, it is not guaranteed that a buffer will be available. If a buffer is not available, the packet fragment will be discarded.

Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard against queue starvation (that is, when a queue does not receive an adequate share of buffers).

Default 180 kilobytes

Parameters *size* — the maximum number of kilobytes (default) or bytes of buffering allowed for the reassembly queue. Entering the **default** keyword returns the MBS rate to the default value of 180 kbytes.

Values 0 to 131072000 | default

bytes — specifies that *size* is measured in bytes

kilobytes — specifies that *size* is measured in kilobytes

wait

Syntax **wait** *milli-seconds*

Context config>router>reassembly>reassembly-profile

Description This command configures the wait time for the reassembly profile. The wait time specifies the amount of time that the IP reassembly function will wait to reassemble a packet before discarding the collected fragments.

Note: The system checks the reassembly queues every 64 ms in a constant loop, which may cause a maximum of 63 ms variation between the user-configured value and the actual detection time. For example, using the default configuration of 2000 ms, the system may check the reassembly queue timer at 1999 ms, in which case the timeout would not occur during that cycle and would instead take place during the next cycle at 2063 ms.

Default 2000

Parameters *milli-seconds* — the length of the wait time, in milliseconds. Entering the **default** keyword returns the wait time to the default value of 2000 milliseconds.

Values 100 to 60000 | default

route-next-hop-policy

Syntax **route-next-hop-policy**

Context config>router

Description This command enables the context to create Loop-Free Alternate (LFA) Shortest Path First (SPF) policies. LFA SPF policies allow specific criteria, such as admin group and SRLG constraints, to be applied when selecting an LFA backup next hop for a subset of prefixes that resolve to a primary next hop.

abort

Syntax **abort**

Context config>router>route-nh

Description This command discards any changes made to the route next-hop policy template.

begin

Syntax **begin**

Context config>router>route-nh

Description This command enters the mode to create or edit the route next-hop policy template.

commit

Syntax **commit**

Context config>router>route-nh

Description This command saves any changes made to the route next-hop policy template.

template

Syntax [**no**] **template** *template-name*

Context config>router>route-nh

Description This command creates a template to configure the attributes of an LFA SPF policy. When the template is created, it can then be applied to a specific OSPF or IS-IS interface. A policy template can be used in both IS-IS and OSPF to apply the specific criteria to prefixes protected by LFA. Each instance of IS-IS or OSPF can apply the same policy template to one or more interfaces.

Use the **begin** command to create or edit the template attributes. Use the **abort** command to discard any changes made before saving. Use the **commit** command to save the changes.

When the **commit** command is issued, OSPF or IS-IS will re-evaluate the template, and if there are any changes, the protocol will schedule a new LFA SPF to recalculate the LFA next hop for the prefixes associated with the template.

Default no template *template-name*

Parameters *template-name* — the name of the route next-hop policy template, up to 32 characters

exclude-group

Syntax [**no**] **exclude-group** *ip-admin-group-name*

Context config>router>route-nh>template

Description This command configures the admin group constraint in the route next-hop policy template. Each group is entered individually. The command prunes all links belonging to the specified admin group before making the LFA backup next-hop selection for a prefix.

If the same group name is part of both the include-group and **exclude-group** statements, the exclude statement takes precedence.

The admin-group criteria are applied before running the LFA next-hop selection algorithm.

The **no** form of the command deletes the admin group constraint from the route next-hop policy template.

Default no exclude-group *ip-admin-group-name*

Parameters *ip-admin-group-name* — the name of the group, up to 32 characters

include-group

Syntax **include-group** *ip-admin-group-name* [**pref** *preference*]
no include-group *ip-admin-group-name*

Context config>router>route-nh>template

Description This command configures the admin group constraint in the route next-hop policy template. Each group is entered individually. The command instructs the LFA SPF selection algorithm to pick up a subset of LFA next hops among the links that belong to one or more of the specified admin groups. A link that does not belong to at least one of the admin groups is excluded.

However, a link can still be selected if it belongs to one of the groups in an **include-group** statement but also belongs to other groups that are not part of any **include-group** statement in the route next-hop policy.

The **pref** option is used to provide a relative preference for which admin group to select. A lower preference value means that LFA SPF will first attempt to select an LFA backup next hop that is a member of the corresponding admin group. If none is found, then the admin group with the next highest preference value is evaluated. If no preference is configured for an admin group name, it is considered to be the least preferred.

When evaluating multiple **include-group** statements with the same preference, any link that belongs to one or more of the included admin groups can be selected as an LFA next hop. There is no relative preference based on how many of those included admin groups the link is a member of.

If the same group name is part of both the **include-group** and **exclude-group** statements, the exclude statement takes precedence.

The admin-group criteria are applied before running the LFA next-hop selection algorithm.

The **no** form of the command deletes the admin group constraint from the route next-hop policy template.

Default no include-group *ip-admin-group-name*

Parameters *ip-admin-group-name* — the name of the group, up to 32 characters

preference — an integer specifying the relative preference of a group; the lower the value, the higher the preference

Values 1 to 255

Default 255

nh-type

Syntax **nh-type** {**ip** | **tunnel**}
no nh-type

Context config>router>route-nh>template

Description This command configures the next-hop type constraint in the route next-hop policy template. Either a tunnel backup next hop or an IP backup next hop can be selected as the preferred next hop. The default is an IP next hop.

If no LFA next hop of the preferred type is found, the other type will be selected.

When the route next-hop policy template is applied to an IP interface, all prefixes using this interface as a primary next hop will follow the next-hop type preference specified in the template.

The **no** form of the command deletes the next-hop type constraint from the route next-hop policy template.

Default no nh-type

Parameters **ip** — specifies that an IP next hop is the preferred backup next hop (default)

tunnel — specifies that a tunnel next hop is the preferred backup next hop

protection-type

Syntax **protection-type** {**link** | **node**}
no protection-type

Context config>router>route-nh>template

Description This command configures the protection type constraint in the route next-hop policy template. Either link protection or node protection can be selected as the preferred protection type in the selection of an LFA next hop for all IP prefixes and LDP FEC prefixes to which the template is applied. The default is node protection.

If no LFA next hop of the preferred type is found, the other type will be selected.

When the route next-hop policy template is applied to an IP interface, all prefixes using this interface as a primary next hop will follow the protection type preference specified in the template.

The **no** form of the command deletes the next-hop type constraint from the route next-hop policy template.

Default no protection-type

Parameters **link** — specifies that link protection is preferred

node — specifies that node protection is preferred (default)

srlg-enable

Syntax [**no**] **srlg-enable**

Context config>router>route-nh>template

Description This command configures the SRLG constraint in the route next-hop policy template. When this command is applied to a prefix, the LFA SPF will attempt to select an LFA next hop that uses an outgoing interface that does not participate in any of the SRLGs of the outgoing interface used by the primary next hop.

The SRLG criterion is applied before running the LFA next-hop selection algorithm.

The **no** form of the command deletes the SRLG constraint from the route next-hop policy template.

Default no srlg-enable

router-id

Syntax **router-id** *ip-address*
no router-id

Context config>router

Description This command configures the router ID for the router instance.

The router ID is used by OSPF and BGP in the routing table manager. IS-IS uses the router ID as its system ID. Refer to the 7705 SAR Routing Protocols Guide for information on OSPF, IS-IS, and BGP.

When configuring a new router ID, protocols are not automatically restarted with the new router ID. The next time a protocol is initialized, the new router ID is used. This can result in an interim period when different protocols use different router IDs.

To force the new router ID to be used, issue the **shutdown** and **no shutdown** commands for each protocol that uses the router ID, or restart the entire router.

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

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

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

service-prefix

Syntax **service-prefix** {*ip-prefix/ip-prefix-length* | *ip-prefix netmask*} [**exclusive**]
no service-prefix {*ip-prefix/ip-prefix-length* | *ip-prefix netmask*}

Context config>router

Description This command reserves one or more IP address ranges for IES or VPRN services. The range can be made up of IPv4 or IPv6 addresses.

When the service is configured, the IP address must be within one of the ranges defined in the **service-prefix** command. If the **service-prefix** command is not configured, then no limitation exists.

Addresses in the range of a service prefix are allocated to a network port unless the **exclusive** parameter is used. Then, the address range is reserved exclusively for services.

When the configured range is a superset of a previously defined service prefix, the new superset definition replaces the existing definition. For example, if a service prefix exists for 10.10.10.0/24, and a new service prefix is configured as 10.10.0.0/16, then the 10.10.10.0/24 service prefix definition is replaced by the new 10.10.0.0/16 service prefix configuration.

Similarly, when the configured range is a subset of a previously defined service prefix, the new subset definition replaces the existing definition providing the addresses used by services are not affected. For example, if a service prefix exists for 10.10.0.0/16, and a new service prefix is configured as 10.10.10.0/24, then the 10.10.0.0/16 entry is removed provided that there are no configured services that are using the 10.10.x.x addresses other than 10.10.10.x.

The **no** form of the command removes all IP address reservations. A service prefix cannot be unreserved if one or more services is using an address or addresses in the defined range.

Default no service-prefix

Parameters *ip-prefix/prefix-length* — the IP address prefix to include in the service prefix allocation, in dotted decimal notation

Values	*ipv4-prefix*	a.b.c.d (host bits must be 0)
	ipv4-prefix-length	0 to 32
Values	*ipv6-prefix*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	ipv6-prefix-length	0 to 128

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)

exclusive — specifies that the addresses configured are for the exclusive use of services and cannot be assigned to network ports

static-route-entry

Syntax **static-route-entry** {*ip-prefix*|*prefix-length*} [**mcast**]

Context config>router

Description This command creates IPv4 and IPv6 static route entries for network routes. When configuring a static route, the **next-hop**, **indirect**, or **black-hole** command, indicating the type of static route, must be configured. Multiple types of static routes **(next-hop**, **indirect**, **black-hole**) can be applied to the same IP prefix. If a static route that is forwarding traffic goes down, the default route will be used instead.

When editing an existing static route—that is, configuring a static-route entry having an existing prefix, subnet mask, and next-hop IP address—the options that were applied before the edit persist unless explicitly changed.

The **no** form of the command deletes the static route entry. If a static route needs to be removed when multiple static routes exist to the same destination, as many parameters as necessary to uniquely identify the static route must be entered. Before deleting the static-route entry, the underlying next-hop, black-hole, or indirect entries need to be **shutdown** and deleted as well. Otherwise, attempting to delete the static-route entry results in the warning "Cannot delete static-route prefix without deleting configured next-hops".

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

The following adapter cards and platforms support the full IPv6 subnet range for IPv6 static routes:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card, version 2 and version 3
- 2-port 10GigE (Ethernet) Adapter card (on the v-port)
- 10-port 1GigE/1-port 10GigE X-Adapter card
- 7705 SAR-X

For these cards and platforms, the supported route range for statically provisioned or dynamically learned routes is from /1 to /128.

For all other cards, modules, and ports (including the v-port on the 2-port 10GigE (Ethernet) module), the supported range for statically provisioned or dynamically learned routes is from /1 to /64 or is /128 (indicating a host route).

Default no static-route-entry

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

Values	*ipv4-prefix*	a.b.c.d (host bits must be 0)
	ipv4-prefix-length	0 to 32
Values	*ipv6-prefix*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	ipv6-prefix-length	0 to 128

mcast — indicates that the static route being configured is used for multicast table only

black-hole

Syntax [**no**] **black-hole**

Context config>router>static-route-entry

Description This command specifies that the route is a blackhole route. If the destination address on a packet matches this static route, it will be silently discarded.

Default no black-hole

metric

Syntax [**no**] **metric** *metric*

Context config>router>static-route-entry>black-hole
config>router>static-route-entry>indirect
config>router>static-route-entry>next-hop

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

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

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

The **no** form of this command returns the metric to the default value.

Default 1

Parameters *metric* — specifies the cost metric value

Values 0 to 65535

preference

Syntax [**no**] **preference** *preference*

Context config>router>static-route-entry>black-hole
config>router>static-route-entry>indirect
config>router>static-route-entry>next-hop

Description This command specifies the preference of this static route over routes from different sources such as OSPF, IS-IS, and BGP. The preference is expressed as a decimal integer. A route with a lower preference value is preferred over a route with a higher preference value.

When modifying the preference value of an existing static route, the metric will not be changed unless specified. The **preference** command is also used to prioritize static routes applied to the same prefix. If a blackhole static route has the same preference as another route with the same prefix, the blackhole route takes a lower precedence.

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

Different protocols should not be configured with the same preference. If this occurs, the tiebreaker is according to the route preference defaults listed in Table 19.

Table 19 **Route Preference Defaults by Route Type**

Route Type	Preference	Configurable
Direct attached	0	No
Static routes	5	Yes
OSPF internal	10	Yes
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

The **no** form of this command returns the associated static route preference to its default value.

Default 5

Parameters *preference* — specifies the route preference value

Values 1 to 255

tag

Syntax [**no**] **tag** *tag*

Context config>router>static-route-entry>black-hole
config>router>static-route-entry>indirect
config>router>static-route-entry>next-hop

Description This command adds a 32-bit integer tag to the static route.

The tag value is used in route policies to control distribution of the route into other protocols.

Default no tag

Parameters *tag* — specifies an integer tag value

Values 1 to 4294967295

indirect

Syntax [**no**] **indirect** *ip-address*

Context config>router>static-route-entry

Description This command specifies that the route is indirect and specifies the next-hop IP address used to reach the destination.

The configured *ip-address* is not directly connected to a network configured on this node. The destination can be reachable via multiple paths. The indirect address can be resolved either via a dynamic routing protocol or by another static route.

The *ip-address* configured for the **indirect** parameter must be on the network side of this node and be at least one hop away from the node.

Default no indirect

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

Values	*ipv4-address*	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x: [0 to FFFF]H
		d: [0 to 255]D

tunnel-next-hop

Syntax **tunnel-next-hop**

Context config>router>static-route-entry>indirect

Description This command enables the context to configure the indirect static route to use a tunnel programmed in the tunnel table manager (TTM) for resolving the next hop of the route.

disallow-igp

Syntax [**no**] **disallow-igp**

Context config>router>static-route-entry>indirect>tunnel-next-hop

Description This command determines whether the static route can be resolved via an IGP next hop in the routing table manager (RTM) if no tunnel next hops are found in the TTM.

If enabled, the static route will not be resolved to an available IGP route in the RTM.

The **no** form of the command returns the behavior to the default, which allows the static route to be resolved via an IGP route in the RTM if no tunnel next hop can be found in the TTM.

Default no disallow-igp

resolution

Syntax **resolution** {**any** | **disabled** | **filter**}

Context config>router>static-route-entry>indirect>tunnel-next-hop

Description This command configures the mode for resolving the static route to a tunnel next hop.

Default resolution any

Parameters **any** — the route can be resolved using any active tunnels (in the static route context) in the TTM, following the TTM preference order

disabled — the route cannot be resolved using active tunnels in the TTM; therefore, it can only be resolved via routes in the RTM

filter — the route can be resolved using a subset of active tunnels in the TTM, determined by the **resolution-filter** configuration

resolution-filter

Syntax **resolution-filter**

Context config>router>static-route-entry>indirect>tunnel-next-hop

Description This command configures the subset of tunnel types that can be used in the resolution of the static route next hop.

If one or more tunnel filter criteria are specified, the tunnel type will be selected following the TTM preference order.

ldp

Syntax [**no**] **ldp**

Context config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter

Description This command enables the use of LDP sourced tunnel entries in the TTM to resolve the static route next hop.

The **ldp** value instructs the system to search for an LDP LSP with a FEC prefix corresponding to the address of the indirect next hop. Both an LDP IPv4 FEC and LDP IPv6 FEC can be used as the tunnel next hop. However, only an indirect next hop of the same family (IPv4 or IPv6) as the prefix of the route can use an LDP FEC as the tunnel next hop; for example, an IPv4 prefix can only be resolved to an IPv4 FEC.

Default no ldp

rsvp-te

Syntax [**no**] **rsvp-te**

Context config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter

Description This command enables the use of RSVP-TE sourced tunnel entries in the TTM to resolve the static route next hop.

The **rsvp-te** value instructs the system to search for the best metric RSVP-TE LSP to the address of the indirect next hop. The LSP metric is provided by MPLS in the tunnel table. If there are multiple RSVP-TE LSPs with the same lowest metric, the system selects the LSP with the lowest **tunnel-id**.

A point-to-point auto LSP that is instantiated via an LSP template can be selected in the TTM when **resolution** is set to **any**.

Default no rsvp-te

lsp

Syntax [**no**] **lsp** *lsp-name*

Context config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter>rsvp-te
config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter>sr-te

Description This command restricts the search for a resolving LSP to a specific set of named LSPs. Only those LSPs named in the associated name list will be searched for a match to resolve the static route next hop.

For RSVP-TE, it is recommended that auto LSP names not be specified because the auto-generated name can change if the node reboots, which will blackhole the traffic of the static route.

Parameters *lsp-name* — the name of the LSP to be searched for a valid tunnel to resolve the static route next hop

sr-isis

Syntax [**no**] **sr-isis**

Context config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter

Description This command enables the use of SR-ISIS sourced tunnel entries in the TTM to resolve the static route next hop.

When the **sr-isis** value is enabled, an SR tunnel to the indirect next hop is selected in the TTM from the lowest-numbered IS-IS instance.

Both SR-ISIS IPv4 and SR-ISIS IPv6 tunnels can be used as tunnel next hops. However, only an indirect next hop of the same family (IPv4 or IPv6) as the prefix of the route can use an SR-ISIS tunnel as the tunnel next hop; for example, an IPv4 prefix can only be resolved using an SR-ISIS IPv4 tunnel.

Default no sr-isis

sr-ospf

Syntax [**no**] **sr-ospf**

Context config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter

Description This command enables the use of SR-OSPF sourced tunnel entries in the TTM to resolve the static route next hop.

When the **sr-ospf** value is enabled, an SR tunnel to the indirect next hop is selected in the TTM from OSPF instance 0.

Segment routing is not supported for OSPFv3. Therefore, SR-OSPF tunnels and tunnel next hops are IPv4 only.

Default no sr-ospf

sr-te

Syntax [**no**] **sr-te**

Context config>router>static-route-entry>indirect>tunnel-next-hop>resolution-filter

Description This command enables the use of SR-TE sourced tunnel entries in the TTM to resolve the static route next hop.

The **sr-te** value instructs the system to search for the best metric SR-TE LSP to the address of the indirect next hop. The LSP metric is provided by MPLS in the tunnel table. If there are multiple SR-TE LSPs with the same lowest metric, the system selects the LSP with the lowest **tunnel-id**.

Default no sr-te

next-hop

Syntax **next-hop** {*ip-int-name* | *ip-address* | *ipv6-address*}

Context config>router>static-route-entry

Description This command specifies the directly connected next-hop IP interface name or IP address used to reach the destination. If the next hop is over an unnumbered interface, the interface name of the unnumbered interface can be used.

If the next hop or interface pointing to the next hop changes state (from active to inactive or vice versa), an event is generated and a trap is raised. The generation of this event is disabled by default. To enable generation of this event globally (across all routing instances), the appropriate command must be configured under **config>log>event-control** (refer to the 7705 SAR System Management Guide).

Default no next-hop

Parameters *ip-address* | *ip-int-name* | *ipv6-address* — the IPv4 or IPv6 address, or interface name of the next hop. The IPv4 or IPv6 address configured for the **next-hop** parameter 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.

The *ip-int-name* 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	*ip-int-name*	1 to 32 characters (must start with a letter)
	ipv4-address	a.b.c.d

ipv6-address	x:x:x:x:x:x:x:x[-*interface*] (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d[-*interface*] x: [0 to FFFF]H d: [0 to 255]D *interface*: 32 characters max, mandatory for link local addresses

bfd-enable

Syntax [**no**] **bfd-enable**

Context config>router>static-route-entry>next-hop

Description This command associates the static route state to a BFD session between the local system and the configured next hop.

The remote end of the BFD session must also be configured to originate or accept the BFD session controlling the static route state.

The **no** form of this command removes the association of the static route state to the BFD session.

Default no bfd-enable

ldp-sync

Syntax [**no**] **ldp-sync**

Context config>router>static-route-entry>next-hop

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

Default no ldp-sync

3.11.2.1.3 Local DHCP and DHCPv6 Server Commands

dhcp

Syntax **dhcp**

Context config>router
config>service>vprn

Description This command enables the context to configure local DHCP server parameters.

dhcp6

Syntax **dhcp6**

Context config>router
config>service>vprn

Description This command enables the context to configure local DHCPv6 server parameters.

local-dhcp-server

Syntax **local-dhcp-server** *server-name* [**create**]
no local-dhcp-server *server-name*

Context config>router>dhcp
config>router>dhcp6
config>service>vprn>dhcp
config>service>vprn>dhcp6

Description This command creates a local DHCP or DHCPv6 server instance. A local DHCP or DHCPv6 server can serve multiple interfaces but is limited to the routing context in which it was created.

The **no** form of the command removes the local DHCP or DHCPv6 server instance.

Default n/a

Parameters *server-name* — the name of the local DHCP or DHCPv6 server

Values up to 32 alphanumeric characters

create — keyword is mandatory when creating a local DHCP or DHCPv6 server

force-renews

Syntax [**no**] **force-renews**

Context config>router>dhcp>local-dhcp-server
config>service>vprn>dhcp>local-dhcp-server

Description This command enables the sending of FORCERENEW messages. If the DHCP server sends a unicast FORCERENEW message to the client, upon receipt of the message, the client will change its state to the RENEW state and will then try to renew its lease according to normal DHCP procedures.

The **no** form of the command disables the use of FORCERENEW messages.

Default no force-renews

ignore-rapid-commit

Syntax [**no**] **ignore-rapid-commit**

Context config>router>dhcp6>local-dhcp-server
config>service>vprn>dhcp6>local-dhcp-server

Description This command specifies whether the Rapid Commit Option (RCO) sent by the DHCPv6 client is processed.

If enabled and the client has included an RCO in the solicit, then the server ignores the option and processes the remainder of the message as if no RCO were present.

The **no** form of the command disables the **ignore-rapid-commit** command.

lease-hold-time

Syntax **lease-hold-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-hold-time

Context config>router>dhcp6>local-dhcp-server
config>service>vprn>dhcp6>local-dhcp-server

Description This command configures the time to retain a lease. The **lease-hold-time** is for unsolicited release conditions such as lease timeout and for normal solicited release from a DHCPv6 client.

Default sec 0

Parameters *days* — the number of days in the lease hold time

Values 0 to 3650

hours — the number of hours in the lease hold time

Values 0 to 23

minutes — the number of minutes in the lease hold time

Values 0 to 59

seconds — the number of seconds in the lease hold time

Values 0 to 59

pool

Syntax **pool** *pool-name* [**create**]
no pool *pool-name*

Context config>router>dhcp>local-dhcp-server
config>router>dhcp6>local-dhcp-server
config>service>vprn>dhcp>local-dhcp-server
config>service>vprn>dhcp6>local-dhcp-server

Description This command configures a DHCP or DHCPv6 address pool on the router.

The **no** form of the command deletes a configured IP address pool.

Default n/a

Parameters *pool-name* — the name of the IP address pool

Values up to 32 alphanumeric characters

create — keyword is mandatory when creating a pool

max-lease-time

Syntax **max-lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no max-lease-time

Context config>router>dhcp>local-dhcp-server>pool
config>service>vprn>dhcp>local-dhcp-server>pool

Description This command configures the maximum amount of time that a client can lease the IP address.

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

Default 10 days

Parameters *days* — the maximum lease time in days

Values 0 to 3650

hours — the maximum lease time in hours

Values 0 to 23

minutes — the maximum lease time in minutes

Values 0 to 59

seconds — the maximum lease time in seconds

Values 0 to 59

min-lease-time

Syntax **min-lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no min-lease-time

Context config>router>dhcp>local-dhcp-server>pool
config>service>vprn>dhcp>local-dhcp-server>pool

Description This command configures the minimum amount of time that a client can lease the IP address.

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

Default 10 days

Parameters *days* — the minimum lease time in days

Values 0 to 3650

hours — the minimum lease time in hours

Values 0 to 23

minutes — the minimum lease time in minutes

Values 0 to 59

seconds — the minimum lease time in seconds

Values 0 to 59

minimum-free

Syntax **minimum-free** *minimum-free* [**percent**] [**event-when-depleted**]
no minimum-free

Context config>router>dhcp>local-dhcp-server>pool
config>router>dhcp>local-dhcp-server>pool>subnet
config>service>vprn>dhcp>local-dhcp-server>pool
config>service>vprn>dhcp>local-dhcp-server>pool>subnet

Description This command configures the minimum number of free addresses in the pool or subnet. If the actual number of free addresses in the pool or subnet falls below the configured minimum, a notification is generated.

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

Default 1

Parameters *minimum-free* — the minimum number of free addresses in the pool or subnet

Values 0 to 255

percent — specifies that the value is a percentage, rather than a decimal value

event-when-depleted — when enabled, triggers a system-generated event when all available addresses in the pool are depleted

offer-time

Syntax **offer-time** [**min** *minutes*] [**sec** *seconds*]
no offer-time

Context config>router>dhcp>local-dhcp-server>pool
config>service>vprn>dhcp>local-dhcp-server>pool

Description This command configures the time interval during which a DHCP offer advertisement is valid. If the client does not respond with a DHCP REQUEST within this interval, the lease is returned to the available lease pool.

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

Default 1 min

Parameters *minutes* — the offer time in minutes

Values 0 to 10

seconds — the offer time in seconds

Values 0 to 59

options

Syntax **options**

Context config>router>dhcp>local-dhcp-server>pool
config>router>dhcp>local-dhcp-server>pool>subnet
config>router>dhcp6>local-dhcp-server>pool
config>router>dhcp6>local-dhcp-server>pool>prefix
config>service>vprn>dhcp>local-dhcp-server>pool
config>service>vprn>dhcp>local-dhcp-server>pool>subnet
config>service>vprn>dhcp6>local-dhcp-server>pool
config>service>vprn>dhcp6>local-dhcp-server>pool>prefix

Description This command enables the context to configure pool options. If the same options are defined several times in different contexts, the options defined at the subnet level take precedence over those defined at the pool level; options defined at the pool level take precedence over those defined from a DHCP or DHCPv6 client request.

custom-option

Syntax **custom-option** *option-number* **address** *ip-address* [*ip-address*...(up to 4 max)]
custom-option *option-number* **address** *ipv6-address* [*ipv6-address*...(up to 4 max)]
custom-option *option-number* **domain** *domain-string*
custom-option *option-number* **hex** *hex-string*
custom-option *option-number* **string** *ascii-string*
no custom-option *option-number*

Context config>router>dhcp>local-dhcp-server>pool>options
config>router>dhcp>local-dhcp-server>pool>subnet>options
config>router>dhcp6>local-dhcp-server>pool>options
config>router>dhcp6>local-dhcp-server>pool>prefix>options
config>service>vprn>dhcp>local-dhcp-server>pool>options
config>service>vprn>dhcp>local-dhcp-server>pool>subnet>options
config>service>vprn>dhcp6>local-dhcp-server>pool>options
config>service>vprn>dhcp6>local-dhcp-server>pool>prefix>options

Description This command configures specific DHCP or DHCPv6 options. If the same options are defined several times in different contexts, the options defined at the subnet level take precedence over those defined at the pool level; options defined at the pool level take precedence over those defined from a DHCP or DHCPv6 client request.

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

Default n/a

Parameters *option-number* — the option number that the DHCP or DHCPv6 server uses to send the identification strings to the DHCP or DHCPv6 client

Values 1 to 254

ip-address — the IPv4 address of the host. Up to four IP addresses can be entered per custom DHCP option.

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

ipv6-address — the IPv6 address of the host. Up to four IPv6 addresses can be entered per custom DHCPv6 option.

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

hex-string — the hex value of this option

Values 0x0 to 0xFFFFFFFF

ascii-string — the value of the option as an ASCII string

Values maximum 127 characters

domain-string — the domain name for the client as an ASCII string (**domain** applies to DHCPv6 only)

Values maximum 127 characters

dns-server

Syntax **dns-server** *ip-address* [*ip-address*...(up to 4 max)]
dns-server *ipv6-address* [*ipv6-address*...(up to 4 max)]

Context config>router>dhcp>local-dhcp-server>pool>options
config>router>dhcp6>local-dhcp-server>pool>options
config>router>dhcp6>local-dhcp-server>pool>prefix>options
config>service>vprn>dhcp>local-dhcp-server>pool>options
config>service>vprn>dhcp6>local-dhcp-server>pool>options
config>service>vprn>dhcp6>local-dhcp-server>pool>prefix>options

Description This command configures the IP address of the DNS servers.

Parameters *ip-address* — the IP address of the DNS server in dotted-decimal notation. Up to four IP addresses can be entered.

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

ipv6-address — the IPv6 address of the host. Up to four IP addresses can be entered per custom DHCPv6 option.

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

domain-name

Syntax **domain-name** *domain-name*
no domain-name

Context config>router>dhcp>local-dhcp-server>pool>options
config>router>dhcp6>local-dhcp-server>pool>options
config>router>dhcp6>local-dhcp-server>pool>prefix>options
config>service>vprn>dhcp>local-dhcp-server>pool>options
config>service>vprn>dhcp6>local-dhcp-server>pool>options
config>service>vprn>dhcp6>local-dhcp-server>pool>prefix>options

Description This command configures the default domain for a DHCP or DHCPv6 client that the router uses to complete unqualified host names (without a dotted-decimal domain name).

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

Parameters *domain-name* — the domain name for the client as an ASCII string

Values maximum 127 characters

lease-rebind-time

Syntax **lease-rebind-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-rebind-time

Context config>router>dhcp>local-dhcp-server>pool>options
config>service>vprn>dhcp>local-dhcp-server>pool>options

Description This command configures the time from the assignment of the IP address until the client transitions to a rebinding state.

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

Default n/a

Parameters *days* — the lease rebinding time in days

Values 0 to 3650

hours — the lease rebinding time in hours

Values 0 to 23

minutes — the lease rebinding time in minutes

Values 0 to 59

seconds — the lease rebinding time in seconds

Values 0 to 59

lease-renew-time

Syntax **lease-renew-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-renew-time

Context config>router>dhcp>local-dhcp-server>pool>options
config>service>vprn>dhcp>local-dhcp-server>pool>options

Description This command configures the time from the assignment of the IP address until the client transitions to a renew state.

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

Default n/a

Parameters *days* — the lease renewal time in days

Values 0 to 3650

hours — the lease renewal time in hours

Values 0 to 23

minutes — the lease renewal time in minutes

Values 0 to 59

seconds — the lease renewal time in seconds

Values 0 to 59

lease-time

Syntax **lease-time** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no lease-time

Context config>router>dhcp>local-dhcp-server>pool>options
config>service>vprn>dhcp>local-dhcp-server>pool>options

Description This command configures the time that the DHCP server grants permission to the DHCP client to use a particular IP address.

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

Default n/a

Parameters *days* — the IP address lease time in days

Values 0 to 3650

hours — the IP address lease time in hours

Values 0 to 23

minutes — the IP address lease time in minutes

Values 0 to 59

seconds — the IP address lease time in seconds

Values 0 to 59

netbios-name-server

Syntax **netbios-name-server** *ip-address* [*ip-address*...(up to 4 max)]
no netbios-name-server

Context config>router>dhcp>local-dhcp-server>pool>options
config>service>vprn>dhcp>local-dhcp-server>pool>options

Description This command configures up to four Network Basic Input/Output System (NetBIOS) name server IP addresses.

The **no** form of this command removes the configuration.

Parameters *ip-address* — the IP address of the NetBIOS name server in dotted-decimal notation. Up to four IP addresses can be entered.

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

netbios-node-type

Syntax **netbios-node-type** {**B** | **P** | **M** | **H**}
no netbios-node-type

Context config>router>dhcp>local-dhcp-server>pool>options
config>service>vprn>dhcp>local-dhcp-server>pool>options

Description This command configures the NetBIOS node type. The available types are:

- B (0x01 broadcast)
- P (0x02 peer; WINS only)
- M (0x04 mixed; broadcast then WINS)
- H (0x08 hybrid; WINS then broadcast)

The **no** form of this command removes the configuration.

Default n/a

Parameters **B** — broadcast node uses broadcasting to query nodes on the network for the owner of a NetBIOS name

P — peer-to-peer node uses directed calls to communicate with a known NetBIOS name server for the IP address of a NetBIOS machine name

M — mixed node uses a broadcast query to find a node, and if that fails, queries a known P-node name server for the address

H — hybrid node is the opposite of the M-node action so that a directed query is executed first, and if that fails, a broadcast query is attempted

prefix

Syntax **prefix** *ipv6-address*/*prefix-length* [**pd**] [**wan-host**] [**create**]
no prefix *ipv6-address*/*prefix-length*

Context config>router>dhcp6>local-dhcp-server>pool
config>service>vprn>dhcp6>local-dhcp-server>pool

Description This command enables a prefix to be routed to hosts associated with the DHCPv6 server pool. Each prefix is represented in the associated FIB with a reference to the pool.

Default n/a

Parameters *ipv6-address* — the base IPv6 address

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

prefix-length — the length of any associated aggregate prefix

Values 1 to 128

pd — specifies that the prefix is used by IPv6 Enhanced Subscriber Management (ESM) hosts for DHCPv6 prefix delegation

wan-host — specifies that the prefix is used by IPv6 ESM hosts for local addressing or by a routing gateway WAN interface

create — keyword is mandatory when creating a prefix entry

preferred-lifetime

Syntax **preferred-lifetime days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no preferred-lifetime

Context config>router>dhcp6>local-dhcp-server>pool>prefix
config>service>vprn>dhcp6>local-dhcp-server>prefix>pool

Description This command configures the preferred lifetime that this prefix will continue to be preferred. The address generated from a prefix that is no longer preferred should not be used as a source address in new communications. However, packets received on such an interface are processed as expected.

Default n/a

Parameters *days* — the preferred lifetime in days

Values 0 to 3650

hours — the preferred lifetime in hours

Values 0 to 23

minutes — the preferred lifetime in minutes

Values 0 to 59

seconds — the preferred lifetime in seconds

Values 0 to 59

rebind-timer

Syntax **rebind-timer** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no rebind-timer

Context config>router>dhcp6>local-dhcp-server>pool>prefix
config>service>vprn>dhcp6>local-dhcp-server>pool>prefix

Description This command configures the time from the assignment of the IP address until the client transitions to a rebinding state.

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

Default n/a

Parameters *days* — the rebinding time in days

Values 0 to 3650

hours — the rebinding time in hours

Values 0 to 23

minutes — the rebinding time in minutes

Values 0 to 59

seconds — the rebinding time in seconds

Values 0 to 59

renew-timer

Syntax **renew-timer** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no renew-timer

Context config>router>dhcp6>local-dhcp-server>pool>prefix
config>service>vprn>dhcp6>local-dhcp-server>pool>prefix

Description This command configures the time from the assignment of the IP address until the client transitions to a renew state.

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

Default n/a

Parameters *days* — the renewal time in days

Values 0 to 3650

hours — the renewal time in hours

Values 0 to 23

minutes — the renewal time in minutes

Values 0 to 59

seconds — the renewal time in seconds

Values 0 to 59

valid-lifetime

Syntax **valid-lifetime** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no valid-lifetime

Context config>router>dhcp6>local-dhcp-server>pool>prefix
config>service>vprn>dhcp6>local-dhcp-server>pool>prefix

Description This command specifies the length of time that the prefix is valid for the purpose of onlink determination. The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

Default n/a

Parameters *days* — the valid lifetime in days

Values 0 to 3650

hours — the valid lifetime in hours

Values 0 to 23

minutes — the valid lifetime in minutes

Values 0 to 59

seconds — the valid lifetime in seconds

Values 0 to 59

subnet

Syntax **subnet** {*ip-address/mask* | *ip-address netmask*} [**create**]
no subnet {*ip-address/mask* | *ip-address netmask*}

Context config>router>dhcp>local-dhcp-server>pool
config>service>vprn>dhcp>local-dhcp-server>pool

Description This command creates a subnet of IP addresses to be served from the pool. The subnet cannot include any addresses that were assigned to subscribers; those addresses must be excluded. When the subnet is created, no IP addresses are made available until a range is defined.

The **no** form of this command removes the configuration.

Default n/a

Parameters *ip-address* — the base IP address of the subnet in dotted-decimal notation

Values a.b.c.d (no multicast address; host bits must be 0)

mask — the subnet mask in Classless Inter-Domain Routing (CIDR) notation, expressed as a decimal integer

Values 8 to 30

netmask — the IP netmask in dotted-decimal notation for the subnet

Values a.b.c.d

create — keyword is mandatory when creating a subnet

address-range

Syntax [**no**] **address-range** *start-ip-address end-ip-address*

Context config>router>dhcp>local-dhcp-server>pool>subnet
config>service>vprn>dhcp>local-dhcp-server>pool>subnet

Description This command configures a range of IP addresses to be served from the pool. All IP addresses between the start and end IP addresses will be included (other than specific excluded addresses).

The **no** form of this command removes the configuration.

Default n/a

Parameters *start-ip-address* — the start IPv4 address of this range. The address must be unique within the subnet and specified in dotted-decimal notation.

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

end-ip-address — the end IPv4 address of this range. The address must be unique within the subnet and specified in dotted-decimal notation

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

exclude-addresses

Syntax [**no**] **exclude-addresses** *start-ip-address* [*end-ip-address*]

Context config>router>dhcp>local-dhcp-server>pool>subnet
config>service>vprn>dhcp>local-dhcp-server>pool>subnet

Description This command configures a range of IP addresses to be excluded from this subnet's pool of IP addresses.

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

Default n/a

Parameters *start-ip-address* — the start IPv4 address of this range. The address must be unique within the subnet and specified in dotted-decimal notation.

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

end-ip-address — the end IPv4 address of this range. The address must be unique within the subnet and specified in dotted-decimal notation

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

maximum-declined

Syntax **maximum-declined** *maximum-declined*
no maximum-declined

Context config>router>dhcp>local-dhcp-server>pool>subnet
config>service>vprn>dhcp>local-dhcp-server>pool>subnet

Description This command configures the maximum number of addresses that the client can decline from the server due to the address being in use.

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

Default 64

Parameters *maximum-declined* — the maximum number of declined addresses allowed

Values 0 to 4294967295

default-router

Syntax **default-router** *ip-address* [*ip-address*...(up to 4 max)]
no default-router

Context config>router>dhcp>local-dhcp-server>pool>subnet>options
config>service>vprn>dhcp>local-dhcp-server>pool>subnet>options

Description This command configures the IP address of the default router for a DHCP client. Up to four IP addresses can be specified.

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

Default n/a

Parameters *ip-address* — the IP address of the default router. The address must be unique within the subnet and specified in dotted-decimal notation.

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

subnet-mask

Syntax **subnet-mask** *ip-address*
no subnet-mask

Context config>router>dhcp>local-dhcp-server>pool>subnet>options
config>service>vprn>dhcp>local-dhcp-server>pool>subnet>options

Description This command specifies the subnet mask option to the client. The mask can either be defined (for supernetting) or taken from the pool address.

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

Default n/a

Parameters *ip-address* — the IP address of the subnet mask. The address must be unique within the subnet and specified in dotted-decimal notation.

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

use-gi-address

Syntax [**no**] **use-gi-address**

Context config>router>dhcp>local-dhcp-server
config>service>vprn>dhcp>local-dhcp-server

Description This command enables the use of gateway IP address (GIADDR) matching. If the gi-address flag is enabled, a pool can be used even if a subnet is not found.

A pool can include multiple subnets. Since the GIADDR is shared by multiple subnets in a subscriber interface, the pool may provide IP addresses from any of the subnets included when the GIADDR is matched to any of its subnets. This allows a pool to be created that represents a subnet.

The **no** form of the command disables GIADDR matching.

Default no use-gi-address

server-id

Syntax **server-id duid-en hex** *hex-string*
server-id duid-en string *ascii-string*
server-id duid-ll
no server-id

Context config>router>dhcp6>local-dhcp-server
config>service>vprn>dhcp6>local-dhcp-server

Description This command allows an operator to customize the **server-id** attribute of a DHCPv6 message from the DHCPv6 proxy server (such as DHCPv6 advertise and reply). By default, the **server-id** uses DUID-ll (DHCP unique identifier-leased line) derived from the system link layer address. Operators have the option to use a unique identifier by using DUID-en (vendor identifier based on enterprise number). There is a maximum length associated with the customizable *hex-string* and *ascii-string*.

Default duid-ll (DUID leased line)

Parameters **duid-ll** — specifies that the DUID system ID is derived from the system link layer address

duid-en — specifies that the DUID system ID is derived from a vendor identifier based on enterprise number

ascii-string — specifies a DUID system ID in ASCII format, up to 58 characters (maximum)

hex-string — specifies a DUID system ID in hexadecimal format, 0x0 to 0xFFFFFFFF (116 hexadecimal nibbles, maximum)

use-link-address

Syntax **use-link-address** [**scope** *scope*]
no use-link-address

Context config>router>dhcp6>local-dhcp-server
config>service>vprn>dhcp6>local-dhcp-server

Description This command enables the local DHCPv6 server to use the link address supplied by the Relay agent to find a matching subnet prefix.

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

Default no use-link-address

Parameters *scope* — specifies the scope of the link address selection

Values subnet | pool

Default subnet

use-pool-from-client

Syntax [**no**] **use-pool-from-client**

Context config>router>dhcp>local-dhcp-server
config>router>dhcp6>local-dhcp-server
config>service>vprn>dhcp>local-dhcp-server
config>service>vprn>dhcp6>local-dhcp-server

Description This command enables the use of the pool indicated by the DHCP or DHCPv6 client. When enabled, the IP address pool to be used by this server is the pool indicated by the vendor-specific suboption 13 of DHCP option 82. When disabled or if there is no suboption 13 in the DHCP message, the pool selection is specified by the value of the GIADDR.

The **no** form of the command disables the use of the pool indicated by the DHCP or DHCPv6 client.

Default no use-pool-from-client

user-ident

Syntax **user-ident** *user-ident*
no user-ident

Context config>router>dhcp6>local-dhcp-server
config>service>vprn>dhcp6>local-dhcp-server

Description This command specifies which method is used by the local DHCPv6 server to uniquely identify a user.

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

Default user-ident duid

Parameters *user-ident* — configures the user identification method

Values duid | interface-id | interface-id-link-local

Default duid

3.11.2.1.4 Router BFD Commands

bfd

Syntax **bfd**

Context config>router

Description This command enables the context to configure global BFD session commands on the router.

Default n/a

bfd-template

Syntax **bfd-template** *name*
no bfd-template

Context config>router>bfd

Description This command creates or edits a BFD template for a router. A BFD template defines the set of parameters used by a BFD session. These parameters include the transmit and receive timers used for BFD continuity check (CC) packets, the transmit timer interval used when the session is providing a connection verification (CV) function, the multiplier value, and whether the BFD session terminates in the network processor.

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

Default no bfd-template

Parameters *name* — the name of the template, up to 32 characters

multiplier

Syntax **multiplier** *multiplier*
no multiplier

Context config>router>bfd>bfd-template

Description This command specifies the integer used during a BFD session to determine when the far end is down. If a BFD control packet is not received for a period of *multiplier* x *receive-interval*, the session is declared down.

The **no** form of the command resets the multiplier to the default value.

Default 3

Parameters *multiplier* — the multiplier for the BFD session

Values 3 to 20

receive-interval

Syntax **receive-interval** *receive-interval*
no receive-interval

Context config>router>bfd>bfd-template

Description This command specifies the interval between received BFD packets that is required to maintain the BFD session.

The **no** form of the command resets the interval to the default value.

Default 100

Parameters *receive-interval* — the receive interval in milliseconds. The minimum interval that can be configured is hardware-dependent.

Values 10 ms to 100000 ms in 1-ms intervals

transmit-interval

Syntax **transmit-interval** *transmit-interval*
no transmit-interval

Context config>router>bfd>bfd-template

Description This command specifies the interval between transmitted BFD packets that is required to maintain the BFD session.

The **no** form of the command resets the interval to the default value.

Default 100

Parameters *transmit-interval* — the transmit interval for the BFD session. The minimum interval that can be configured is hardware-dependent.

Values 10 ms to 100000 ms in 1-ms intervals

type

Syntax **type np**
no type

Context config>router>bfd>bfd-template

Description This command sets the CSM network processor as the local termination point for the BFD session. This setting is enabled by default.

Default np

seamless-bfd

Syntax **seamless-bfd**

Context config>router>bfd

Description This command enables the context to configure global seamless BFD (S-BFD) initiator parameters on this router.

Default n/a

peer

Syntax [**no**] **peer** {*ip-address* | *ipv6-address*}

Context config>router>bfd>seamless-bfd

Description This command creates the context for the local mapping between a far-end S-BFD reflector and its discriminator value. The mapping is used by the router when it is acting as an S-BFD initiator.

For IPv6, only a global unicast address can be used as a peer address.

The **no** form of this command removes the peer address from the mapping table.

Default n/a

Parameters *ip-address* — the IPv4 address of the peer

Values a.b.c.d

ipv6-address — the IPv6 address of the peer

Values

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

discriminator

Syntax **discriminator** *discriminator*
no discriminator

Context config>router>bfd>seamless-bfd>peer

Description This command specifies the S-BFD reflector discriminator for the remote peer in the mapping table that is used for S-BFD sessions initiated by the router.

The **no** form of this command removes the discriminator.

Default n/a

Parameters *discriminator* — the discriminator of the remote router

Values 1 to 4294967295

3.11.2.1.5 Seamless BFD Reflector Commands

seamless-bfd

Syntax **seamless-bfd**

Context config>bfd

Description This command enables the context to configure the parameters for a seamless BFD (S-BFD) reflector on the router.

Default n/a

reflector

Syntax **reflector** *reflector-name*
no reflector

Context config>bfd>seamless-bfd

Description This command configures the S-BFD reflector name.

The **no** form of this command removes the reflector.

Default n/a

Parameters *reflector-name* — the reflector name, up to 32 characters

description

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

Context config>bfd>seamless-bfd>reflector

Description This command configures a description for the S-BFD reflector.

The **no** form of this command removes the description.

Default n/a

Parameters *description-string* — the S-BFD reflector description, up to 80 characters

discriminator

Syntax **discriminator** *discriminator*
no discriminator

Context config>bfd>seamless-bfd>reflector

Description This command configures the discriminator for the S-BFD reflector. The S-BFD discriminator must be unique for each router and separate from the BFD discriminators negotiated by standard BFD sessions. The discriminator value is configured from a defined range.

The **no** form of this command removes the discriminator.

Default n/a

Parameters *discriminator* — the discriminator value

Values 0x80000 to 0x807FF (or 524288 to 526335)

local-state

Syntax **local-state** {**admin-down** | **up**}
no local-state

Context config>bfd>seamless-bfd>reflector

Description This command sets the local state field in reflected S-BFD control packets.

The **no** form of this command means that the field is not explicitly set by the reflector.

Default up

Parameters **admin-down** — the local state of the reflected S-BFD control packets is administratively down. The reflector continues to reflect packets but initiators must transmit at a maximum rate of 1 packet/s.

up — the local state of the reflected S-BFD control packets is up

shutdown

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

Context config>bfd>seamless-bfd>reflector

Description This command specifies the administrative state of the seamless BFD reflector.

The **no** form of this command administratively enables the reflector. A discriminator must be configured before the **no shutdown** command is issued.

Default shutdown

3.11.2.1.6 Router Interface Commands

interface

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

Context config>router

Description This command creates a logical IP routing interface. When 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 interface

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 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* | **dhcp**} [**client-identifier** [*ascii-value* | **interface-name**]] [**vendor-class-id** *vendor-class-id*]
no address

Context config>router>interface

Description This command assigns an IP address and IP subnet to an IP interface or enables the interface to accept a dynamic IP address using DHCP. 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. Interface- specific configurations for MPLS/RSVP-TE are also removed. This will operationally stop any MPLS LSPs that explicitly reference that IP address.

When a new IP address is defined, interface-specific configurations for MPLS/RSVP-TE must be added again.

If dynamic IP address assignment is enabled (using the **dhcp** keyword), the DHCP client ID (Option 61) and vendor class ID (Option 60) can be configured as specified in RFC 2132.

Default no address

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)

dhcp — specifies that the IP address is assigned dynamically using DHCP

client-identifier *ascii-value* **| interface-name** — the DHCP client ID, either an ASCII string or the interface name; each client attached to a subnet must have a unique identifier. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. If the **interface-name** is specified, the system uses the MAC address of the interface.

Values *ascii-value* — an ASCII string up to 64 characters (as per RFC 2132)
interface-name — hexadecimal MAC address (as per RFC 2132)

vendor-class-id — the DHCP vendor class ID that identifies the vendor type and configuration of the DHCP client as a variable-length string of octets. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values an ASCII string up to 64 characters (as per RFC 2132)

allow-directed-broadcasts

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

Context config>router>interface

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

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

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

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

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

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

Default no allow-directed broadcasts

arp-retry-timer

Syntax **arp-retry-timer** *ms-timer*
no arp-retry-timer

Context config>router>interface

Description This command specifies the length of time, in 100s of milliseconds, that the system waits before reissuing a failed ARP request.

The **no** form of the command resets the interval to the default value.

Note: The ARP retry default value of 5000 ms is intended to protect CPU cycles on the 7705 SAR, especially when it has a large number of interfaces. Configuring the ARP retry timer to a value shorter than the default should be done only on mission-critical links, such as uplinks or aggregate spoke SDPs transporting mobile traffic; otherwise, the retry interval should be left at the default value.

Default 50 (in 100s of ms)

Parameters *ms-timer* — the time interval, in 100s of milliseconds, the system waits before retrying a failed ARP request

Values 1 to 300

arp-timeout

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

Context config>router>interface

Description This command configures the minimum interval, in seconds, that an ARP entry learned on the IP interface is stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host. Otherwise, the ARP entry is aged from the ARP table. If the **arp-timeout** value is set to 0 s, ARP aging is disabled.

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

Note: The 7705 SAR will attempt to refresh an ARP entry 30 s prior to its expiry. This refresh attempt occurs only if the ARP timeout is set to 45 s or more.

Default no arp-timeout

Parameters *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 s (4 h)

bfd

Syntax **bfd** *transmit-interval* [**receive** *receive-interval*] [**multiplier** *multiplier*] [**type np**]
no bfd

Context config>router>interface
config>router>if>ipv6

Description This command configures the time interval in which BFD control messages are transmitted and received on the interface. The *multiplier* parameter specifies the number of consecutive BFD messages that must be missed by the peer node before the BFD session closes and the upper layer protocols (OSPF, IS-IS, BGP, PIM) are notified of the fault.

See Bidirectional Forwarding Detection (BFD) for more information on BFD.

Default no bfd

Parameters *transmit-interval* — the number of milliseconds between consecutive BFD sent messages

Values 10 to 100000

Default 100

receive-interval — the number of milliseconds between consecutive BFD received messages

Values 10 to 100000

Default 100

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

Values 3 to 20

Default 3

type np — controls the value range of the *transmit-interval* and *receive-interval* parameters. If the **type np** option is not specified, the range of the *transmit-interval* and *receive-interval* parameter values is from 100 ms to 100000 ms. If the **type np** option is specified, the range of the *transmit-interval* and *receive-interval* parameter values is from 10 ms to 1000 ms, with the restriction that the maximum receiving detection time for the missing BFD packets must be less than or equal to 3000 ms. The maximum receiving detection time is the *receive-interval* parameter multiplied by the *multiplier* parameter.

Note: The BFD session must be disabled before the **type np** parameter can be changed.

cflowd-parameters

Syntax **cflowd-parameters**

Context config>router>interface

Description This command enables the context to configure Cflowd parameters for the specified IP interface.

Cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement.

Default n/a

sampling

Syntax **sampling** {**unicast** | **multicast**} **type** {**interface**} [**direction** {**ingress-only** | **egress-only** | **both**}]
no sampling {**unicast** | **multicast**}

Context config>router>if>cflowd-parameters

Description This command configures the Cflowd sampling behavior to collect traffic flow samples through a router for analysis.

This command can be used to configure the sampling parameters for unicast and multicast traffic separately.

If Cflowd sampling is enabled with no **direction** parameter specified, **ingress-only** sampling is enabled by default.

The **no** form of the command disables the configured type of traffic sampling on the interface.

Default no sampling unicast

no sampling multicast

Parameters **unicast** — Cflowd will sample unicast traffic on the interface

multicast — Cflowd will sample multicast traffic on the interface

interface — specifies that all traffic entering or exiting the interface is subject to sampling

direction — specifies the direction in which to collect traffic flow samples: **ingress-only**, **egress-only**, or **both** directions

if-attribute

Syntax **if-attribute**

Context config>router>interface

Description This command enables the context to assign interface attributes such as administrative group and SRLG.

admin-group

Syntax [**no**] **admin-group** *group-name* [*group-name*...(up to 5 max)]

Context config>router>if>if-attribute

Description This command associates admin groups with this interface. The admin group must already be defined in the **config>router>if-attribute**>admin-group context.

Up to five groups can be specified with one command. When an admin group is bound to one or more interfaces, its value cannot be changed until all bindings are removed.

When admin groups are associated with network IP interfaces, the interfaces can be included or excluded in the route next-hop selection by matching on the admin-group name in a route next-hop policy template applied to an interface or a set of prefixes.

The configured admin-group membership is applied in all levels or areas that the interface is participating in. The same interface cannot have different memberships in different levels or areas.

The **no** form of this command deletes the association of this interface with one or more of the admin groups.

Default no admin-group

Parameters *group-name* — specifies the name of the admin group. The group names should be the same across all routers in the IP domain.

srlg-group

Syntax [**no**] **srlg-group** *group-name* [*group-name*...(up to 5 max)]

Context config>router>if>if-attribute

Description This command associates SRLGs with this interface. The SRLG must already be defined in the **config>router>if-attribute**>srlg-group context.

Up to five SRLGs can be specified with one command. When an SRLG is bound to one or more interfaces, its value cannot be changed until all bindings are removed.

When SRLGs are associated with network IP interfaces, they are evaluated in the route next-hop selection if the **srlg-enable** option is included in a route next-hop policy template applied to an interface or a set of prefixes. For example, the SRLG constraint can be enabled to select an LFA next hop for a prefix that avoids all interfaces that share the same outcome as the primary next hop.

The configured SRLG membership is applied in all levels or areas that the interface is participating in. The same interface cannot have different memberships in different levels or areas.

The **no** form of this command deletes the association of this interface with one or more of the SRLGs.

Default n/a

Parameters *group-name* — specifies the name of the SRLG. The SRLG names should be the same across all routers in the IP domain.

ldp-sync-timer

Syntax **ldp-sync-timer** *seconds*
no ldp-sync-timer

Context config>router>interface

Description This command configures the IGP-LDP synchronization timer to enable synchronization of IGP and LDP and synchronization of static routes and LDP. This command is not supported on RIP interfaces.

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

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

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

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

If the user changes the cost of an interface, the new value is advertised at the next flooding of link attributes by IGP. However, if the LDP synchronization timer is still running, the new cost value will only be advertised after the timer expires. Also, if the currently advertised cost is different, the new cost value will be advertised after the user executes any of the following commands:

- **tools>perform>router>ospf>ldp-sync-exit**
- **tools>perform>router>isis>ldp-sync-exit**
- **config>router>interface>no ldp-sync-timer**
- **config>router>ospf>disable-ldp-sync**
- **config>router>isis>disable-ldp-sync**

Refer to the 7705 SAR OAM and Diagnostics Guide for the tools commands and to the 7705 SAR Routing Protocols Guide for the OSPF and IS-IS commands.

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

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

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

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

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

Default no ldp-sync-timer

Parameters *seconds* — the time interval for the IGP-LDP synchronization timer

Values 1 to 800

load-balancing

Syntax **load-balancing**

Context config>router>interface

Description This command enables the context to configure load balancing hashing options on the interface. The options enabled at the interface level overwrite parallel system-level configurations.

Default n/a

l4-load-balancing

Syntax **l4-load-balancing** *hashing-algorithm*
no l4-load-balancing

Context config>router>interface>load-balancing

Description This command configures Layer 4 load balancing at the interface level. Configuration must be done on the ingress network interface (that is, the interface on the node that the packet is received on). When enabled, Layer 4 source and destination port fields of incoming TCP/UDP packets are included in the hashing calculation to randomly determine the distribution of packets.

You can add additional fields to generate more randomness and more equal distribution of packets with the teid-load-balancing command.

The default configuration on the interface is to match the Layer 4 load-balancing configuration in the **config>system** context. Using this command to modify Layer 4 load-balancing configuration on an interface overrides the system-wide load-balancing settings for that interface.

Parameters *hashing-algorithm* — specifies whether Layer 4 source and destination port fields are included in the hashing calculation

Values **includeL4**: include Layer 4 source and destination port fields in the hashing calculation

excludeL4: exclude Layer 4 source and destination port fields in the hashing calculation

Default the system configuration setting (under **config>system** context)

lsr-load-balancing

Syntax **lsr-load-balancing** *hashing-algorithm* [**bottom-of-stack** *hashing-treatment*] [**use-ingress-port**]
no lsr-load-balancing

Context config>router>interface>load-balancing

Description This command configures LSR load balancing at the interface level. Configuration must be done on the ingress network interface (that is, the interface on the LDP LSR node that the packet is received on).

Hashing can be enabled on the IP header at an LSR to send labeled packets over multiple equal-cost paths in an LDP LSP and/or over multiple links of a LAG group in all types of LSPs.

The **bottom-of-stack** option determines the significance of the bottom-of-stack label (VC label) based on which label stack profile option is specified.

When LSR load balancing is enabled, the default configuration for the hashing algorithm is label-only (**lbl-only**) hashing, and the default configuration for the bottom-of-stack hashing treatment is **profile-1**.

The **use-ingress-port** option, when enabled, specifies that the ingress port will be used by the hashing algorithm at the LSR. This option should be enabled for ingress LAG ports because packets with the same label stack can arrive on all ports of a LAG interface. In this case, using the ingress port in the hashing algorithm will result in better egress load balancing, especially for pseudowires.

The option should be disabled for LDP ECMP so that the ingress port is not used by the hashing algorithm. For ingress LDP ECMP, if the ingress port is used by the hashing algorithm, the hash distribution could be biased, especially for pseudowires.

LSR load-balancing configuration on an interface overrides the system-wide LSR load-balancing settings for the interface.

Default no lsr-load-balancing

Parameters *hashing-algorithm* — specifies the hashing algorithm

Values

lbl-only	hashing is done on the MPLS label stack, up to a maximum of 10 labels
lbl-ip	hashing is done on the MPLS label stack and the IPv4 source and destination IP address if an IPv4 header is present after the MPLS labels
lbl-ip-l4-teid	hashing is done on the MPLS label stack, the IPv4 source and destination IP address (if present), then on the Layer 4 source and destination UDP or TCP port fields (if present) and the TEID in the GTP header (if present)

Default lbl-only

hashing-treatment — specifies which label stack profile option to use; profiles determine the significance of the bottom-of-stack label (VC label)

Values

profile-1	favors better load balancing for pseudowires when the VC label distribution is contiguous
profile-2	similar to profile-1 where the VC labels are contiguous, but provides an alternate distribution
profile-3	all labels have equal influence in hash key generation

Default profile-1

use-ingress-port — when configured, specifies that the ingress port is used by the hashing algorithm at the LSR

spi-load-balancing

Syntax [**no**] **spi-load-balancing**

Context config>router>interface>load-balancing

Description This command enables SPI hashing for ESP/AH encrypted IPv4 or IPv6 traffic at the interface level.

The **no** form of this command disables SPI hashing.

Default no spi-load-balancing

teid-load-balancing

Syntax [**no**] **teid-load-balancing**

Context config>router>interface>load-balancing

Description This command configures TEID load balancing at the interface level. Configuration must be done on the ingress network interface (that is, the interface on the node that the packet is received on). The TEID attribute is included in the header of GTP (general packet radio system tunneling protocol) packets. When TEID load balancing is enabled, the TEID field of incoming TCP/UDP packets is included in the hashing calculation to randomly determine the distribution of packets.

You can add additional fields to generate more randomness and more equal distribution of packets with the l4-load-balancing command.

Default no teid-load-balancing

local-dhcp-server

Syntax [**no**] **local-dhcp-server** *local-server-name*

Context config>router>interface

Description This command associates the interface with a local DHCP server configured on the system.

The **no** form of the command removes the association of the interface with the local DHCP server.

Default n/a

Parameters *local-server-name* — the name of the local DHCP server

Values up to 32 alphanumeric characters

local-proxy-arp

Syntax [**no**] **local-proxy-arp**

Context config>router>interface

Description This command enables local proxy ARP on the interface.

Local proxy ARP allows the 7705 SAR to respond to ARP requests received on an interface for an IP address that is part of a subnet assigned to the interface. The router responds to all requests for IP addresses within the subnet with its own MAC address and forwards all traffic between the hosts in the subnet.

Local proxy ARP is used on subnets where hosts are prevented from communicating directly.

Default no local-proxy-arp

loopback

Syntax [**no**] **loopback**

Context config>router>interface

Description This command configures the interface as a loopback interface.

Default no loopback

mac

Syntax **mac** *ieee-address*
no mac

Context config>router>interface

Description This command assigns a specific MAC address to the network interface.

The **no** form of the command returns the MAC address to the default value.

Default IP interface has a system-assigned MAC address

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

multicast-translation

Syntax [**no**] **multicast-translation**

Context config>router>interface

Description This command enables multicast address translation on the 7705 SAR that is the translator router for unicast-to-multicast or multicast-to-multicast translation.

When enabled for unicast-to-multicast translation, the 7705 SAR will try to find the source and destination address of the packet in the unicast-to-multicast translation table. If the source and destination address is not found, the packet is processed as a regular IP packet. To disable unicast-to-multicast translation, all entries must be removed from the translation table and then the command must be set to **no multicast-translation**.

When enabled for multicast-to-multicast translation, the static group configuration is used for multicast PDUs that arrive on the node and are to be translated via the translation table. If the command is enabled and an arriving PDU does not match an entry in the translation table, the multicast PDU is dropped. If the (S,G) arrives from another interface via a dynamic protocol while this command is enabled, the interface that the dynamic (S,G) arrived from will be added as an outgoing interface but it will not forward traffic. Only the outgoing loopback interface on the translation router will forward the translated PDU.

For multicast-to-multicast translation, if this command is not enabled, the node will function as a leaf for the static group configuration.

To disable multicast-to-multicast translation, the interface must be shut down before the **no** version of this command is issued.

Default no multicast-translation

ntp-broadcast

Syntax [**no**] **ntp-broadcast**

Context config>router>interface

Description This command enables or disables the receiving of SNTP broadcasts on the IP interface.

This parameter is only valid when the SNTP **broadcast-client** global parameter is configured.

The **no** form of the command disables SNTP broadcast received on the IP interface.

Default no ntp-broadcast

port

Syntax **port** *port-name*
no port

Context config>router>interface

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

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

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

The port name consists of the *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 (PPP or IMA). Refer to the 7705 SAR Interface Configuration Guide for information on configuring ports.

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

Default no port

Parameters *port-name* — the physical port identifier, in the form *port-id*[:*encap-val*]

Values *encap-val* 0 (for null)
0 to 4094 (for dot1q)

port-id — the physical port identifier

Values *slot/mda/port*[.*channel*]

bundle-id	bundle-*type-slot/mda.bundle-num*	
	bundle	keyword
	type	ima, ppp
	bundle-num	1 to 32
aps-id	aps-*group-id*[.*channel*]	
	aps	keyword
	group-id	1 to 24
mw-link-id	mw-link-*link-num*	
	link-num	1 to 24

proxy-arp-policy

Syntax **proxy-arp-policy** *policy-name* [*policy-name*...(up to 5 max)]
no proxy-arp-policy

Context config>router>interface

Description This command enables proxy ARP on the interface and specifies an existing policy statement that controls the flow of routing information by analyzing match and action criteria. The policy statement is configured in the **config>router>policy-options** context (see Route Policy Options in the Route Policy Command Reference section). When proxy ARP is enabled, the 7705 SAR responds to ARP requests on behalf of another device.

Default no proxy-arp-policy

Parameters *policy-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. The policy statement must already be defined.

qos

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

Context config>router>interface

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

reassembly-profile

Syntax [**no**] **reassembly-profile** *profile-id*

Context config>router>interface

Description This command assigns a reassembly profile to the interface. The same interface must receive all fragments from a fragmented flow.

Reassembly profiles cannot be assigned to an interface that uses an unsupported adapter card, or to a LAG that contains a port from an unsupported adapter card. All Ethernet adapter cards and Ethernet ports on the 7705 SAR fixed platforms support reassembly profiles except for the following adapter cards:

- 2-port 10GigE (Ethernet) Adapter card
- 8-port Ethernet Adapter card

The **no** form of the command removes the association between the interface and the reassembly profile.

Default no reassembly-profile

Parameters *profile-id* — the identification number of the IP reassembly profile; the profile must already exist

Values 1 to 16

remote-proxy-arp

Syntax [**no**] **remote-proxy-arp**

Context config>router>interface

Description This command enables remote proxy ARP on the interface, allowing a router on one network to respond to ARP requests intended for another node that is physically located on another network. The router effectively pretends to be the destination node by sending an ARP response to the originating node that associates the router's MAC address with the destination node's IP address (acts as a proxy for the destination node). The router then takes responsibility for routing traffic to the real destination.

Default no remote-proxy-arp

static-arp

Syntax **static-arp** *ip-addr ieee-mac-addr*
no static-arp *ip-addr*
static-arp *ieee-mac-addr* **unnumbered**
no static-arp unnumbered

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.

Static ARP is used when a 7705 SAR needs to know about a device on an interface that cannot or does not respond to ARP requests. Therefore, the 7705 SAR 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-arp

Parameters *ip-addr* — the IP address for the static ARP in 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.

unnumbered — specifies the static ARP MAC addresses for an unnumbered interface. Unnumbered interfaces also support dynamic ARP. If this parameter is configured, it overrides any dynamic ARP.

tcp-mss

Syntax **tcp-mss** *value*
no tcp-mss

Context config>router>interface
config>router>if>ipv6

Description This command configures the maximum segment size (MSS) in a TCP SYN or SYN-ACK packet during the establishment of a TCP connection. A **tcp-mss** value can be specified on an ingress interface, egress interface, or both. When configured on two interfaces, the smaller of the two values is used. If the TCP SYN packet has no TCP MSS field, the 7705 SAR assigns it the MSS value configured on the interface and recalculates the IP checksum. If the TCP SYN or SYN-ACK packet has an MSS field and the value is greater than the value configured on the interface, the 7705 SAR overwrites the packet MSS value with the lower value. If the MSS value is less than the value configured on the interface, the packet MSS value does not change.

This command is supported on interfaces with IPv4 and IPv6 traffic, and a different MSS value can be configured for the IPv4 and IPv6 interfaces.

Default no tcp-mss

Parameters *value* — the MSS, in bytes, to be used in a TCP SYN or SYN-ACK packet

Values 384 to 9732

unnumbered

Syntax **unnumbered** [*ip-int-name* | *ip-address*] [**dhcp**] [**client-identifier** *ascii-value* | **interface-name**] [**vendor-class-id** *vendor-class-id*]
no unnumbered

Context config>router>interface

Description This command configures an IP interface as an unnumbered interface and specifies an IP address or interface name to be used for the interface. Unnumbered interfaces are point-to-point interfaces that are not explicitly configured with a dedicated IP address and subnet; instead, they borrow an IP address from another interface on the system (the system IP address, another loopback interface, or any other numbered interface).

If the **dhcp** keyword is specified, the interface can accept a dynamic system IP address using DHCP. If dynamic IP address assignment is enabled, the DHCP client ID (Option 61) and vendor class ID (Option 60) can be configured as specified in RFC 2132.

Only one unnumbered interface with the **dhcp** option can be associated with the “system” interface. Attempts to configure a second unnumbered interface with a binding to “system” is blocked in the CLI when the “system” interface already has an “unnumbered dhcp” binding.

Only one IP address can be associated with an IP interface; the interface cannot be configured as unnumbered if an IP address already exists.

By default, no IP address 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. Interface- specific configurations for MPLS are also removed. This will operationally stop any MPLS LSPs that explicitly reference that IP address.

When a new IP address is defined, interface-specific configurations for MPLS must be added again.

Default no unnumbered

Parameters *ip-int-name* | *ip-address* — the IP interface name or address to associate with the unnumbered IP interface. It is recommended that the system IP address be used because it is not associated with a particular interface and is therefore always reachable.

Values *ip-int-name*: 1 to 32 characters (must start with a letter)
ip-address: a.b.c.d

Default system IP address

dhcp — specifies that the IP address is assigned dynamically using DHCP

client-identifier *ascii-value* **| interface-name** — the DHCP client ID, either an ASCII string or the interface name; each client must have a unique identifier. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. If the **interface-name** is specified, the system uses the MAC address of the interface.

Values *ascii-value* — an ASCII string up to 64 characters (as per RFC 2132)
interface-name — hexadecimal MAC address (as per RFC 2132)

vendor-class-id — the DHCP vendor class ID that identifies the vendor type and configuration of the DHCP client as a variable-length string of octets. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values an ASCII string up to 64 characters (as per RFC 2132)

3.11.2.1.7 Router Interface IPv6 Commands

ipv6

Syntax [**no**] **ipv6**

Context config>router>interface

Description This command enables the context to configure IPv6 parameters on a router interface.

IP version 6 (IPv6) addresses are supported on:

- access ports (IES and VPRN)
- network ports (null or dot1q encapsulation) on:
  - 2-port 10GigE (Ethernet) Adapter card (v-port only)
  - 8-port Ethernet Adapter card
  - 6-port Ethernet 10Gbps Adapter card
  - 8-port Gigabit Ethernet Adapter card
  - 10-port 1GigE/1-port 10GigE X-Adapter card
  - Packet Microwave Adapter card
  - Ethernet ports on the 7705 SAR-M
  - Ethernet ports on the 7705 SAR-A
  - Ethernet ports on the 7705 SAR-Ax
  - 7705 SAR-W
  - Ethernet ports on the 7705 SAR-Wx
  - 7705 SAR-H
  - Ethernet ports on the 7705 SAR-Hc
  - Ethernet ports on the 7705 SAR-X
  - Ethernet management port
  - 2-port 10GigE (Ethernet) module (v-port only)
  - 4-port SAR-H Fast Ethernet module
  - 6-port SAR-M Ethernet module
- network ports on the 4-port OC3/STM1 Clear Channel Adapter card (POS encapsulation)

This command automatically generates an FE80:: link-local address.

The **no** form of the command disables IPv6 on the interface.

Default no ipv6

address

Syntax **address** *ipv6-address/prefix-length* [**eui-64**] [**preferred**]
no address *ipv6-address/prefix-length*

Context config>router>if>ipv6

Description This command assigns an IPv6 address to the interface.

The following adapter cards and platforms support the full IPv6 subnet range for interface IP addresses:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card, version 2 and version 3
- 2-port 10GigE (Ethernet) Adapter card (on the v-port)
- 10-port 1GigE/1-port 10GigE X-Adapter card
- 7705 SAR-X

For these cards and platforms, the supported interface IP address prefixes are from /4 to /127, and /128 on system or loopback interfaces.

For all other cards, modules, and ports (including the v-port on the 2-port 10GigE (Ethernet) module), the supported interface IP address prefixes are from /4 to /64, and /128 on system or loopback interfaces.

Default n/a

Parameters *ipv6-address/prefix-length* — the IPv6 address on the interface

Values	*ipv6-address*	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x: [0 to FFFF]H
		d: [0 to 255]D
	prefix-length	{4 to 128} | {4 to 64 | 128}

eui-64 — when the **eui-64** keyword is specified, a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. If a port has not been assigned to the interface, the 64-bit interface identifier is derived from the system MAC address and does not change after a port is added. The same behavior applies for the link-local address.

preferred — specifies that the IPv6 address is the preferred IPv6 address for this interface. A preferred address is an address assigned to an interface whose use by upper layer protocols is unrestricted. A preferred address may be used as the source or destination address of packets sent from or to the interface.

local-dhcp-server

Syntax [**no**] **local-dhcp-server** *local-server-name*

Context config>router>if>ipv6

Description This command associates the interface with a local DHCPv6 server configured on the system.

The **no** form of the command removes the association of the interface with the local DHCPv6 server.

Default n/a

Parameters *local-server-name* — the name of the local DHCPv6 server

Values up to 32 alphanumeric characters

link-local-address

Syntax **link-local-address** *ipv6-address* [**preferred**]
no link-local-address

Context config>router>if>ipv6

Description This command configures the IPv6 link-local address.

The **no** form of the command removes the configured link-local address, and the router automatically generates a default link-local address.

Removing a manually configured link-local address may impact routing protocols that have a dependency on that address.

Default n/a

Parameters *ipv6-address* — the IPv6 address

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

preferred — specifies that the IPv6 address is the preferred IPv6 address for this interface. A preferred address is an address assigned to an interface whose use by upper layer protocols is unrestricted. A preferred address may be used as the source or destination address of packets sent from or to the interface.

neighbor

Syntax **neighbor** *ipv6-address mac-address*
no neighbor *ipv6-address*

Context config>router>if>ipv6

Description This command configures an IPv6-to-MAC address mapping on the interface. Use this command if a directly attached IPv6 node does not support ICMPv6 neighbor discovery or a static address must be used. This command can only be used on Ethernet interfaces. The *ipv6-address* must be on the subnet that was configured from the IPv6 address command or a link-local address.

Parameters *ipv6-address* — the IPv6 address on the interface

Values	*ipv6-address*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	mac-address	the MAC address for the neighbor in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx

reachable-time

Syntax **reachable-time** *seconds*
no reachable-time

Context config>router>if>ipv6

Description This command specifies the time that an IPv6 neighbor remains in a reachable state.

Default no reachable-time

Parameters *seconds* — the number of seconds that an IPv6 neighbor remains in a reachable state

Values 30 to 3600

Default 30

stale-time

Syntax **stale-time** *seconds*
no stale-time

Context config>router>if>ipv6

Description This command specifies the time that an IPv6 neighbor cache entry remains in a stale state on a router. When the specified time elapses, the system removes the neighbor cache entry.

Default no stale-time

Parameters *seconds* — the number of seconds that an IPv6 neighbor remains in stale state

Values 60 to 65535

Default 14400

3.11.2.1.8 Router Interface DHCP Relay Agent Commands

dhcp

Syntax **dhcp**

Context config>router>interface

Description This command enables the context to configure DHCP Relay Agent parameters.

gi-address

Syntax **gi-address** *ip-address* [**src-ip-addr**]
no gi-address

Context config>router>if>dhcp

Description This command configures the gateway interface address for the DHCP Relay Agent. By default, the GIADDR used in the relayed DHCP packet is the primary address of an interface.

Default no gi-address

Parameters *ip-address* — the IP address of the gateway interface in dotted-decimal notation

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

src-ip-addr — specifies that the GIADDR is to be used as the source IP address for DHCP relay packets

option

Syntax [**no**] **option**

Context config>router>if>dhcp

Description This command enables DHCP Option 82 (Relay Agent Information Option) parameters processing and enters the context for configuring Option 82 suboptions.

The **no** form of this command returns the system to the default.

Default no option

action

Syntax **action** {**replace** | **drop** | **keep**}
no action

Context config>router>if>dhcp>option

Description This command configures the processing required when the 7705 SAR receives a DHCP request that already has a Relay Agent Information Option (Option 82) field in the packet.

The **no** form of this command returns the system to the default value.

Default keep (as per RFC 3046, *DHCP Relay Agent Information Option*, section 2.1.1, Reforwarded DHCP requests, the default is to keep the existing information intact. The exception to this occurs if the gi-addr (gateway interface address) of the received packet is the same as the ingress address on the router. In this case, the packet is dropped and an error is logged.)

Parameters **replace** — in the upstream direction (from the user), the existing Option 82 field is replaced with the Option 82 field from the router. In the downstream direction (towards the user) the Option 82 field is stripped (in accordance with RFC 3046).

drop — the packet is dropped, and an error is logged

keep — the existing information is kept in the packet and the router does not add any additional information. In the downstream direction, the Option 82 field is not stripped and is sent on towards the client. If no Option 82 field is present, the router will not create the Option 82 field.

circuit-id

Syntax **circuit-id** [**ascii-tuple** | **port-id** | **if-name**]
no circuit-id

Context config>router>if>dhcp>option

Description When enabled, the router sends the interface index (If Index) in the **circuit-id** suboption of the DHCP packet. The If Index of a router interface can be displayed using the **show>router> interface>detail** command. This option specifies data that must be unique to the router that is relaying the circuit.

If disabled, the **circuit-id** suboption of the DHCP packet will be left empty.

The **no** form of this command returns the system to the default.

Default ascii-tuple

Parameters **ascii-tuple** — specifies that the ASCII-encoded concatenated “tuple” will be used, where “tuple” consists of the *system name, interface name, and port ID*, separated by the syntax symbol “|”.

port-id — specifies that the port identifier will be used. The port identifier can be displayed using the command **show>router>interface>detail**.

if-name — specifies that the interface name will be used

copy-82

Syntax [**no**] **copy-82**

Context config>router>if>dhcp>option

Description This command copies the DHCP Option 82 into Option 43 (vendor-specific) on the DHCP offer destined for the DHCP client. This command is used in conjunction with the Auto-Discovery Protocol to allow the Auto-Discovery client node to learn about its network uplink.

The **no** form of this command returns the system to the default.

Default no copy

remote-id

Syntax **remote-id** [**mac** | **string** *string*]
no remote-id

Context config>router>if>dhcp>option

Description When enabled, the router sends the MAC address of the remote end (typically, the DHCP client) in the **remote-id** suboption of the DHCP packet. This command identifies the host at the other end of the circuit. If disabled, the **remote-id** suboption of the DHCP packet will be left empty.

The **no** form of this command returns the system to the default.

Default no remote-id

Parameters **mac** — specifies the MAC address of the remote end is encoded in the suboption

string — specifies the remote ID

Values up to 32 alphanumeric characters

server

Syntax **server** *server1* [*server2...*(up to 8 max)]
no server

Context config>router>if>dhcp

Description This command specifies a list of servers where requests will be forwarded. The list of servers can be entered as either IP addresses or fully qualified domain names. There must be at least one server specified for DHCP Relay to work. If there are multiple servers specified, then the request is forwarded to all of the servers in the list. There can be a maximum of eight DHCP servers configured.

Default no server

Parameters *server* — specifies the DHCP server IP address

3.11.2.1.9 Router Interface Filter Commands

egress

Syntax **egress**

Context config>router>interface

Description This command enables access to the context to configure egress network filter policies for the IP interface.

If an egress filter policy is not defined, no filtering is performed.

ingress

Syntax **ingress**

Context config>router>interface

Description This command enables access to the context to configure ingress network filter policies for the IP interface.

If an ingress filter policy is not defined, no filtering is performed.

agg-rate-limit

Syntax **agg-rate-limit** *agg-rate* [**cir** *cir-rate*]
no agg-rate-limit

Context config>router>if>egress

Description This command sets the aggregate rate limits (PIR and CIR) for the VLAN bound to the network interface once a queue-policy has been assigned. The *agg-rate* sets the PIR value. The *cir-rate* sets the CIR value. On Gen-3 hardware, the *cir-rate* for this command can be configured and is applied but has no effect on the network port. For a network interface on a hybrid port, this command takes effect. For information on adapter card generations, refer to the “Evolution of Ethernet Adapter Cards, Modules, and Platforms” section in the 7705 SAR Interface Configuration Guide.

The **queue-policy** command is used to enable and disable network egress per-VLAN shapers on a per-network-interface basis. If a queue policy has not been assigned, or if the **no queue-policy** command is issued, then the VLAN interface defaults to the unshaped mode and the aggregate rate limits are set to their default values. The **agg-rate-limit** command is only valid when the VLAN shaper is enabled.

Configuring the *cir-rate* is optional. If a *cir-rate* is not entered, then the *cir-rate* is set to its default value (0 kb/s). If a *cir-rate* has been set and the *agg-rate* is changed without re-entering the *cir-rate*, then the *cir-rate* automatically resets to 0 kb/s. For example, to change the *agg-rate* from 2000 to 1500 while maintaining a *cir-rate* of 500, use the command **agg-rate-limit** 1500 **cir** 500.

The **no** form of the command sets the *agg-rate* to the maximum and the *cir-rate* to 0 kb/s.

Default no agg-rate-limit

Parameters *agg-rate* — sets the PIR for the aggregate of all the queues on the VLAN bound to the network interface. The **max** keyword applies the maximum physical port rate possible.

Values 1 to 10000000 kb/s, or **max**

Default max (the default PIR is same as the port egress rate)

cir-rate — sets the CIR for the aggregate of all the queues on the VLAN bound to the network interface. The **max** keyword applies the CIR defined for the physical port.

Values 0 to 10000000 kb/s, or **max**

Default 0 kb/s

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
no filter [**ip** *ip-filter-id* |**ipv6** *ipv6-filter-id*]

Context config>router>if>egress
config>router>if>ingress

Description This command associates an IP filter policy with an IPv4 or IPv6 interface. IPv4 filters are supported on all ingress and egress network interfaces. IPv6 filters are supported on all Ethernet ingress and egress network interfaces (with null or dot1q encapsulation) and on ingress and egress interfaces on the 4-port OC3/STM1 Clear Channel Adapter card (with POS encapsulation).

Filter policies control packet forwarding and dropping based on IP match criteria.

The *ip-filter-id* or *ipv6-filter-id* must have been preconfigured before this **filter** command is executed. If the filter ID does not exist, an error occurs.

Only one filter ID can be assigned to an interface unless the interface is dual-stack (supports both IPv4 and IPv6). A dual-stack interface can have one IPv4 and one IPv6 filter ID assigned to it.

The **no** form of the command removes the filter policy associated with the IP interface.

Default n/a

Parameters *ip-filter-id* — the ID for the IPv4 filter policy expressed as a decimal integer. The filter policy must already exist within the **config>filter>ip-filter** context.

Values 1 to 65535

ipv6-filter-id — the ID for the IPv6 filter policy expressed as a decimal integer. The filter policy must already exist within the **config>filter>ip-filter** context.

Values 1 to 65535

Note: For information on configuring IP filter IDs, see Creating an IPv4 or IPv6 Filter Policy.

queue-policy

Syntax **queue-policy** *name*
no queue-policy

Context config>router>if>egress

Description This command specifies the network queue policy that defines queue parameters such as CBS, MBS, CIR, and PIR rates, as well as forwarding class-to-queue mappings for the shaped VLAN queues. The network queue policy is defined in the **config>qos>network-queue** context. Refer to the 7705 SAR Quality of Service Guide, “Network Queue QoS Policies”, for more information.

The **queue-policy** command is used to enable and disable network egress per-VLAN shapers on a per-network-interface basis. If the VLAN shaper is enabled, then a set of network egress queues is created specifically for the interface, and traffic for that interface is handled by a per-VLAN shaper in the egress direction. If a queue policy has not been assigned, or if the **no queue-policy** command is issued, then the VLAN interface defaults to the unshaped mode and the agg-rate-limit is set to its default values. If the VLAN shaper is disabled for the interface, then the queues created for the interface are deleted, and traffic goes to the unshaped VLAN aggregate queues that are shared by all other interfaces (or VLANs).

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

Default “default”

Parameters *name* — specifies an existing network queue QoS policy name

3.11.2.1.10 Router Interface Encryption Commands

group-encryption

Syntax [**no**] **group-encryption**

Context config>router>interface

Description This command enables network group encryption (NGE) on the router interface. When NGE is enabled on the interface, all received Layer 3 packets that have the protocol ID configured as ESP are considered to be NGE packets and must be encrypted using a valid set of keys from any preconfigured key group on the system.

The **no** form of the command disables NGE on the interface. NGE cannot be disabled unless all key groups and IP exception filters are removed.

Default no group-encryption

encryption-keygroup

Syntax **encryption-keygroup** *keygroup-id* **direction** {**inbound** | **outbound**}
no encryption-keygroup direction {**inbound** | **outbound**}

Context config>router>if>group-encryption

Description This command is used to bind a key group to a router interface for inbound or outbound packet processing. When configured in the outbound direction, packets egressing the router use the **active-outbound-sa** associated with the configured key group. When configured in the inbound direction, received packets must be encrypted using one of the valid security associations configured for the key group.

The **no** form of the command removes the key group from the router interface in the specified direction.

Default no encryption-keygroup direction inbound
no encryption-keygroup direction outbound

Parameters *keygroup-id* — the ID number of the key group being configured

Values 1 to 127 | *keygroup-name* (64 characters maximum)

inbound — binds the key group in the inbound direction

outbound — binds the key group in the outbound direction

ip-exception

Syntax **ip-exception** *filter-id* **direction** {**inbound** | **outbound**}
no ip-exception direction {**inbound** | **outbound**}

Context config>router>if>group-encryption

Description This command associates an IP exception filter policy with an NGE-enabled router interface to allow packets matching the exception criteria to transit the NGE domain as clear text.

When an exception filter is added for inbound traffic, packets matching the criteria in the IP exception filter policy are allowed to be received in clear text even if an inbound key group is configured. If no inbound key group is configured, then associated inbound IP exception filter policies will be ignored.

When an exception filter is added for outbound traffic, packets matching the criteria in the IP exception filter policy are not encrypted when sent out of the router interface even if an outbound key group is configured. If no outbound key group is configured, then associated outbound IP exception filter policies will be ignored.

The **no** form of the command removes the IP exception filter policy from the specified direction.

Default no ip-exception direction inbound
no ip-exception direction outbound

Parameters *filter-id* — specifies the IP exception filter policy. The IP exception ID or exception name must have already been created.

Values 1 to 65535 | *filter-name* (64 characters maximum)

inbound — binds the exception filter policy in the inbound direction

outbound — binds the exception filter policy in the outbound direction

3.11.2.1.11 Router Interface ICMP and ICMPv6 Commands

icmp

Syntax **icmp**

Context config>router>interface

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

mask-reply

Syntax [**no**] **mask-reply**

Context config>router>if>icmp

Description 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 enables the generation of ICMP Time To Live (TTL) expired messages and configures the rate that the 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-s 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 s

Parameters *number* — the maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. The *seconds* parameter must also be specified.

Values 10 to 100

seconds — the interval, in seconds, used to limit the number of ICMP TTL expired messages that can be issued, expressed as a decimal integer

Values 1 to 60

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context config>router>if>icmp

Description This command enables the generation of ICMP host and network destination unreachable messages on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of destination unreachable messages that can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachables messages is enabled at a maximum rate of 100 per 10-s time interval.

The **no** form of the command disables the generation of ICMP destination unreachables on the router interface.

Default unreachables 100 10 — maximum of 100 unreachable messages in 10 s

Parameters *number* — the maximum number of ICMP unreachable messages to send, expressed as a decimal integer. The *seconds* parameter must also be specified.

Values 10 to 100

seconds — the interval, in seconds, used to limit the *number* of ICMP unreachable messages that can be issued, expressed as a decimal integer

Values 1 to 60

icmp6

Syntax **icmp6**

Context config>router>if>ipv6

Description This command enables the context to configure ICMPv6 parameters on an interface.

packet-too-big

Syntax **packet-too-big** [*number seconds*]
no packet-too-big

Context config>router>if>ipv6>icmp6

Description This command enables the generation of ICMPv6 packet-too-big messages and configures the rate that the messages are issued by the IP interface.

The **no** form of the command disables the sending of ICMPv6 packet-too-big messages.

Default 100 10

Parameters *number* — the maximum number of packet-too-big messages to send, expressed as a decimal integer, in the time frame specified by the *seconds* parameter

Values 10 to 1000

seconds — the time frame, in seconds, used to limit the number of packet-too-big messages that can be issued, expressed as a decimal integer

Values 1 to 60

param-problem

Syntax **param-problem** [*number seconds*]
no param-problem

Context config>router>if>ipv6>icmp6

Description This command enables the generation of ICMPv6 param-problem messages and configures the rate that the messages are issued by the IP interface.

The **no** form of the command disables the sending of ICMPv6 param-problem messages.

Default 100 10

Parameters *number* — the maximum number of param-problem messages to send, expressed as a decimal integer, in the time frame specified by the *seconds* parameter

Values 10 to 1000

seconds — the time frame, in seconds, used to limit the number of param-problem messages that can be issued, expressed as a decimal integer

Values 1 to 60

time-exceeded

Syntax **time-exceeded** [*number seconds*]
no time-exceeded

Context config>router>if>ipv6>icmp6

Description This command enables the generation of ICMPv6 time-exceeded messages and configures the rate that the messages are issued by the IP interface.

The **no** form of the command disables the sending of ICMPv6 time-exceeded messages.

Default 100 10

Parameters *number* — the maximum number of time-exceeded messages to send, expressed as a decimal integer, in the time frame specified by the *seconds* parameter

Values 10 to 1000

seconds — the time frame, in seconds, used to limit the number of time-exceeded 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>ipv6>icmp6

Description This command enables the generation of ICMPv6 host and network destination unreachable messages on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *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.

The **no** form of the command disables the generation of ICMPv6 destination unreachables on the router interface.

Default 100 10

Parameters *number* — the maximum number of destination unreachable messages to send, expressed as a decimal integer, in the time frame specified by the *seconds* parameter

Values 10 to 1000

seconds — the time frame, in seconds, used to limit the number of destination unreachable messages that can be issued, expressed as a decimal integer

Values 1 to 60

3.11.2.1.12 Router Advertisement Commands

router-advertisement

Syntax [**no**] **router-advertisement**

Context config>router

Description This command enables the context to configure router advertisement properties. By default, it is disabled for all IPv6-enabled interfaces.

The **no** form of the command disables router advertisement on all IPv6 interfaces.

Default no router-advertisement

interface

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

Context config>router>router-advertisement

Description This command configures router advertisement properties on a specified interface. The interface name must already exist in the **config>router>interface** context.

The **no** form of the command disables router advertisement on the specified router interface.

Default n/a

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 characters (must start with a letter)

current-hop-limit

Syntax **current-hop-limit** *number*
no current-hop-limit

Context config>router>router-advertisement>interface

Description This command configures the current hop limit in the router advertisement messages. It informs the nodes on the subnet about the hop limit when originating IPv6 packets.

Default 64

Parameters *number* — the hop limit

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

managed-configuration

Syntax [**no**] **managed-configuration**

Context config>router>router-advertisement>interface

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

Default no managed-configuration

max-advertisement-interval

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

Context config>router>router-advertisement>interface

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

Default 600

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

Values 4 to 1800

min-advertisement-interval

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

Context config>router>router-advertisement>interface

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

Default 200

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

Values 3 to 1350

mtu

Syntax **mtu** *mtu-bytes*
no mtu

Context config>router>router-advertisement>interface

Description This command configures the MTU for the nodes to use when sending packets on the link.

The **no** form of the command means that the MTU option is not sent in the router advertisement messages.

Default no mtu

Parameters *mtu-bytes* — the MTU for the nodes to use when sending packets

Values 1280 to 9212

other-stateful-configuration

Syntax [**no**] **other-stateful-configuration**

Context config>router>router-advertisement>interface

Description This command sets the “Other configuration” flag. This flag indicates that DHCPv6lite is available for autoconfiguration of other (non-address) information such as DNS-related information or information on other servers in the network. See RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) for IPv6*.

Default no other-stateful configuration

prefix

Syntax **prefix** *ipv6-prefix/prefix-length*
no prefix

Context config>router>router-advertisement>interface

Description This command configures an IPv6 prefix in the router advertisement messages. To support multiple IPv6 prefixes, use multiple prefix statements. No prefix is advertised until it is explicitly configured using prefix statements.

Default n/a

Parameters *ipv6-prefix/prefix-length* — the IPv6 prefix

Values *ipv6-prefix* x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D
prefix-length 4 to 127

autonomous

Syntax [**no**] **autonomous**

Context config>router>router-advertisement>if>prefix

Description This command specifies whether the prefix can be used for stateless address autoconfiguration.

Default autonomous

on-link

Syntax [**no**] **on-link**

Context config>router>router-advertisement>if>prefix

Description This command specifies whether the prefix can be used for onlink determination.

Default on-link

preferred-lifetime

Syntax **preferred-lifetime** [*seconds* | **infinite**]
no preferred-lifetime

Context config>router>router-advertisement>if>prefix

Description This command configures the remaining time, in seconds, that this prefix will continue to be preferred. The address generated from a prefix that is no longer preferred should not be used as a source address in new communications. However, packets received on such an interface are processed as expected.

Default 604800

Parameters *seconds* — the remaining length of time, in seconds, that this prefix will be preferred

Values 1 to 4294967294

infinite — the prefix will always be preferred. A value of 4294967295 represents infinity.

valid-lifetime

Syntax **valid-lifetime** [*seconds* | **infinite**]
no valid-lifetime

Context config>router>router-advertisement>if>prefix

Description This command specifies the length of time, in seconds, that the prefix is valid for the purpose of onlink determination. The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

Default 2592000

Parameters *seconds* — the remaining length of time, in seconds, that this prefix will be valid

Values 1 to 4294967294

infinite — the prefix will always be valid. A value of 4294967295 represents infinity.

reachable-time

Syntax **reachable-time** *milli-seconds*
no reachable-time

Context config>router>router-advertisement>interface

Description This command configures how long the router should be considered reachable by other nodes on the link after receiving a reachability confirmation.

Default no reachable-time

Parameters *milli-seconds* — the length of time that the router should be considered reachable

Values 0 to 3600000

retransmit-time

Syntax **retransmit-time** *milli-seconds*
no retransmit-time

Context config>router>router-advertisement>interface

Description This command configures the retransmission frequency of neighbor solicitation messages.

Default no retransmit-time

Parameters *milli-seconds* — the amount of time that a host should wait before retransmitting neighbor solicitation messages

Values 0 to 1800000

router-lifetime

Syntax **router-lifetime** *seconds*
no router-lifetime

Context config>router>router-advertisement>interface

Description This command configures the router lifetime.

Default no router-lifetime

Parameters *seconds* — the length of time, in seconds (relative to the time that the packet is sent), that the prefix is valid for route determination

Values 0, 4 to 9000 (a value of 0 means that the router is not a default router on this link)

use-virtual-mac

Syntax [**no**] **use-virtual-mac**

Context config>router>router-advertisement>interface

Description This command enables the sending of router advertisement messages using the VRRP virtual MAC address, provided that the virtual router is currently the master.

If the virtual router is not the master, no router advertisement messages are sent.

The **no** form of the command disables the sending of router advertisement messages.

Default no use-virtual-mac

3.11.2.1.13 Router Security Zone Configuration Commands

zone

Syntax **zone** {*zone-id* | *zone-name*} [**create**]
no zone {*zone-id* | *zone-name*}

Context config>router

Description This command creates or specifies a security zone within a router context. Each zone must have a unique identifier.

All zones must be explicitly created with the **create** keyword.

Enter an existing zone without the **create** keyword to edit zone parameters.

The **no** form of this command deletes the zone. When a zone is deleted, all configuration parameters for the zone are also deleted.

Parameters *zone-id* — the zone ID number, from 1 to 65534. The zone ID must be unique within the system.

zone-name — the name of the zone, up to 32 characters (must start with a letter). Zone names must be unique within the system. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

abort

Syntax **abort**

Context config>router>zone

Description This command discards changes made to a security feature.

Default n/a

begin

Syntax **begin**

Context config>router>zone

Description This command enters the mode to create or edit security features.

Default n/a

commit

Syntax **commit**

Context config>router>zone

Description This command saves changes made to security features.

Default n/a

inbound

Syntax **inbound**

Context config>router>zone

Description This command enables the context to configure limit parameters for inbound firewall sessions.

Default n/a

outbound

Syntax **outbound**

Context config>router>zone

Description This command enables the context to configure limit parameters for outbound firewall sessions.

Default n/a

limit

Syntax **limit**

Context config>router>zone>inbound
config>router>zone>outbound

Description This command enables the context to configure limits on concurrent sessions for inbound or outbound firewall sessions.

Default n/a

concurrent-sessions

Syntax **concurrent-sessions** {**tcp** | **udp** | **icmp** | **other**} *sessions*
no concurrent-sessions {**tcp** | **udp** | **icmp** | **other**}

Context config>router>zone>inbound>limit
config>router>zone>outbound>limit

Description This command configures the maximum number of concurrent firewall sessions that can be established per zone, in either the inbound or outbound direction, for the specified protocol.

Default n/a

Parameters **tcp** — specifies that TCP connection traffic is to be firewalled

udp — specifies that UDP connection traffic is to be firewalled

icmp — specifies that ICMP connection traffic is to be firewalled

other — specifies that the traffic to be firewalled is other than TCP, UDP, or ICMP

sessions — the maximum number of concurrent firewall sessions that can be created in a zone for the configured direction and protocol

Values 1 to 16383

interface

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

Context config>router>zone

Description This command creates a logical IP routing interface for a zone. Once created, attributes such as an IP address can be associated with the IP interface. Multiple interfaces can be configured for each zone.

The **no** form of this command removes the IP interface and all the associated configurations.

Parameters *ip-int-name* — the name of the interface to be configured within the zone

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

log

Syntax **log** {*log-id* | *name*}
no log

Context config>router>zone

Description This command applies a security log to the specified zone. The security log must already be configured in the **config>security>logging** context.

The **no** form of this command removes logging for the zone.

Parameters *log-id* — the identifier for the log

Values 1 to 32 characters

name — the name of the log

Values 1 to 32 characters

name

Syntax **name** zone-*name*
no name

Context config>router>zone

Description This command configures a zone name. The zone name is unique within the system. It can be used to refer to the zone under configure, show, and clear commands.

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

Parameters *zone-name* — specifies the name of the zone. Zone names must be unique within the system. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

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

nat

Syntax **nat**

Context config>router>zone

Description This command enters the context to configure NAT parameters for a zone.

pool

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

Context config>router>zone>nat

Description This command configures the NAT pool for a security zone. Each pool must have a unique ID.

All pools must be explicitly created with the **create** keyword.

Enter an existing pool without the **create** keyword to edit pool parameters.

The **no** form of this command deletes the specified NAT pool. When a pool is deleted, all configuration parameters for the pool will also be deleted.

Parameters *pool-id* — the pool ID number

Values 1 to 100

direction

Syntax **direction** {**zone-outbound** | **zone-inbound** | **both**}
no direction

Context config>router>zone>nat>pool

Description This command configures the NAT pool direction for the security zone. A specific NAT pool can be configured for different directions while using the same policy. For example, if the security policy entry direction is set to **both**, separate inbound and outbound pools can be created for that policy.

Parameters **zone-outbound** — configures a pool for the policy outbound traffic

zone-inbound — configures a pool for the policy inbound traffic

both — configures a pool for policy inbound and outbound traffic

entry

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

Context config>router>zone>nat>pool

Description This command configures a NAT pool entry.

The **no** form of this command deletes the entry with the specified ID. When an entry is deleted, all configuration parameters for the entry will also be deleted.

Parameters *entry-id* — the entry ID number

Values 1 to 65535

ip-address

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

Context config>router>zone>nat>pool>entry

Description This command configures the source IP address or IP address range to which packets that match NAT policy are routed using NAT. An interface can also be configured, in which case all packets that match NAT policy are routed to the interface IP address. If the interface IP address is changed dynamically, NAT is updated accordingly. Only one IP address can be associated with an IP interface. Source IP addresses and interfaces cannot be used together in a single NAT pool.

The IP address for the interface must be entered in dotted-decimal notation. The maximum IP address range limit is 255.

Note: A NAT pool interface cannot be an unnumbered interface. A security session will not be created if the NAT pool interface is configured as an unnumbered interface. However, the loopback interface used for an unnumbered interface can be used as a NAT pool interface.

The **no** form of the command removes the IP address assignment. The **no** form of this command can only be performed when the IP interface is administratively shut down. Shutting down the IP interface brings the interface operationally down.

Parameters *ip-address* — the source IP address or address range to be used by NAT. The *ip-address* portion of the **ip-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

ip-int-name — the name of the interface to be used by NAT

port

Syntax **port** *port* [**to** *port*]
no port

Context config>router>zone>nat>pool>entry

Description This command configures the UDP/TCP port or port range. Packets that match NAT policy undergo network port address translation (NPAT) and are routed to their source UDP/TCP port. Configuring a UDP/TCP port pool requires an IP address pool because the 7705 SAR does not support port address translation (PAT) alone.

The **no** form of this command deletes the port or port range.

Parameters *port* — the UDP/TCP port or range of ports to which NPAT is applied

name

Syntax **name** *pool-name*
no name

Context config>router>zone>nat>pool

Description This command configures a zone pool name. Pool names must be unique within the group of pools defined for a zone. A pool name can be used to refer to the pool under configure, show, and clear commands.

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

Parameters *pool-name* — the name of the pool. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

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

policy

Syntax **policy** {*policy-id* | *policy-name*}
no policy

Context config>router>zone

Description This command sets the policy to be used by the security zone to build its matching criteria for incoming packets.

The **no** form of this command deletes the specified policy.

Parameters *policy-id* — the number of the referenced policy

Values 1 to 65535

policy-name — the name of the referenced policy

3.11.2.1.14 Static One-to-One NAT Router Configuration Commands

static-nat-inside

Syntax [**no**] **static-nat-inside**

Context config>router>interface

Description This command configures an interface as an inside (private) interface.

By default, all interfaces are outside (public) interfaces. The **no** form of this command returns the interface to the default setting.

Default no static-nat-inside

static-nat

Syntax [**no**] **static-nat**

Context config>router

Description This command enables the context to configure static one-to-one NAT.

The **no** form of this command disables static one-to-one NAT.

Default no static-nat

drop-packets-without-nat-entry

Syntax [**no**] **drop-packets-without-nat-entry**

Context config>router>static-nat

Description This command configures the router to drop packets traveling from either an inside network to an outside network or an outside network to an inside network that do not have a NAT mapping entry.

By default, packets traveling from either an inside network to an outside network or an outside network to an inside network are forwarded whether or not there is a NAT mapping entry.

The **no** form of this command returns the router to the default behavior.

Default no drop-packets-without-nat-entry

inside

Syntax **inside**

Context config>router>static-nat

Description This command creates a static one-to-one NAT mapping from an inside network to an outside network. When configured, a packet traveling from an inside network to an outside network that matches a NAT mapping entry will have NAT applied to its source IP address. Similarly, a packet traveling from an outside network to an inside network that matches a NAT mapping entry will have NAT applied to its destination IP address.

Default n/a

map

Syntax **map start** *ip-address* **end** *ip-address* **to** *ip-address*
no map start *ip-address* **end** *ip-address*

Context config>router>static-nat>inside

Description This command maps a range of inside source IP addresses that will undergo NAT to a specified outside IP address range.

For example, to map the entire range of inside addresses within 192.168.0.0/16 to the outside address 10.10.0.0/16, the configuration would be:

map start 192.168.0.0 **end** 192.168.255.255 **to** 10.10.0.0

The 7705 SAR will then map each inside source IP address to its corresponding outside IP address sequentially; for example:

- inside address 192.168.0.1 maps to 10.10.0.1
- inside address 192.168.10.10 maps to 10.10.10.10
- inside address 192.168.254.100 maps to 10.10.254.100

The **no** form of this command removes the NAT mapping.

Default no map start *ip-address* end *ip-address*

Parameters **start** *ip-address* — identifies the start of the range of inside IPv4 addresses that will undergo NAT to an outside address, in the format a.b.c.d

end *ip-address* — identifies the end of the range of inside IPv4 addresses that will undergo NAT to an outside address, in the format a.b.c.d

to *ip-address* — identifies the outside IPv4 address that the range of inside addresses maps to, in the format a.b.c.d

shutdown

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

Context config>router>static-nat>inside>map

Description This command administratively disables the static one-to-one NAT map entry.

The **no** form of this command administratively enables the static one-to-one NAT map entry.

Default no shutdown

3.11.2.1.15 TWAMP Light Commands

twamp-light

Syntax **twamp-light**

Context config>router

Description This command enables the context for configuring TWAMP Light functionality.

Default disabled

reflector

Syntax **reflector**

Context config>router>twamp-light

Description This command enables the context for configuring TWAMP Light session reflector functionality. The reflector functionality is enabled using the **no shutdown** command.

Default disabled

prefix

Syntax [**no**] **prefix** *ip-prefix/prefix-length* [**create**]

Context config>router>twamp-light>reflector

Description This command configures an IP address prefix containing one or more TWAMP Light session controllers. It is used to define which TWAMP Light packet prefixes the reflector will process. Once the prefix is configured, the TWAMP Light session reflector only responds to TWAMP Light packets from source addresses that are part of the prefix list.

Default no prefix

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

Values	*ipv4-prefix*	a.b.c.d (host bits must be 0)
	ipv4-prefix-length	0 to 32
	ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	ipv6-prefix-length	{0 to 128} | {0 to 64 | 128}

udp-port

Syntax **udp-port** *number*
no udp-port

Context config>router>twamp-light>reflector

Description This command configures the specific UDP port that the session reflector listens to for TWAMP Light packets. The session controller launching the TWAMP Light packets must have the same UDP port configured as the session reflector.

Default no udp-port

Parameters *number* — the UDP port number

Values 1024 to 65535

3.11.2.2 Show Commands

Note: The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

arp

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

Context show>router

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

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

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

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

ip-address/[mask] — only displays the ARP entry associated with the specified IP address and optional mask

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

summary — displays an abbreviated list of ARP entries

arp-type — only displays ARP information associated with the specified keyword

Values local, dynamic, static, managed

Output The following output is an example of the ARP table, and Table 20 describes the fields.

Output Example

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

*A:ALU-A# show router arp to-ser1
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Expiry      Type Interface
-------------------------------------------------------------------------------

10.10.13.1      04:5b:01:01:00:02 03:53:09    Sta  to-ser1
===============================================================================
*A:ALU-A#
```

Table 20 **ARP Table Field Descriptions**

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

authentication

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

Context show>router>authentication

Description This command displays interface or policy authentication statistics.

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

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

name — specifies an existing policy name

Output The following output is an example of the authentication statistics, and Table 21 describes the fields.

Output Example

```
*A:ALU-1#show>router>auth# statistics
===============================================================
Authentication Global Statistics
===============================================================
Client Packets Authenticate Fail     : 0
Client Packets Authenticate Ok       : 12
===============================================================
*A:ALU-1#
```

Table 21 **Authentication Statistics Field Descriptions**

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

bfd

Syntax **bfd**

Context show>router

Description This command enables the context to display bidirectional forwarding detection (BFD) information.

interface

Syntax **interface**

Context show>router>bfd

Description This command displays BFD interface information.

Output The following output is an example of BFD interface information, and Table 22 describes the fields.

Output Example

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

Table 22 **BFD Interface Field Descriptions**

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

session

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

Context show>router>bfd

Description This command displays session information.

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

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

Output The following output is an example of BFD session information, and Table 23 describes the fields.

Output Example

```
*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
   10.1.2.1                   None                    5029      5029
net1_2_3                      Up (3)                  100       100       3
   10.2.3.2                   None                    156367    156365
-------------------------------------------------------------------------------
No. of BFD sessions: 2
===============================================================================
*A:ALU-1#
```

Table 23 **BFD Session Field Descriptions**

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

dhcp

Syntax **dhcp**

Context show>router

Description This command enables the context to display DHCP-related information.

dhcp6

Syntax **dhcp6**

Context show>router

Description This command enables the context to display DHCPv6-related information.

local-dhcp-server

Syntax **local-dhcp-server** *server-name*

Context show>router>dhcp
show>router>dhcp6

Description This command enables the context to display information about a local DHCP server.

Parameters *server-name* — the name of the local DHCP server

associations

Syntax **associations**

Context show>router>dhcp>local-dhcp-server
show>router>dhcp6>local-dhcp-server

Description This command displays the interfaces associated with this DHCP server.

Output The following output is an example of DHCP server association information, and Table 24 describes the fields.

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server local1 associations
===============================================================================
DHCP server local1 router 3
===============================================================================
Associations                    Admin
-------------------------------------------------------------------------------
sim84                           Up
===============================================================================
*A:ALU-1#
```

Table 24 **DHCP Server Associations Field Descriptions**

Label	Description
Associations	The name of the associated interface
Admin	The administrative state of the interface

declined-addresses

Syntax **declined-addresses** *ip-address*[*/mask*] [**detail**]
declined-addresses pool *pool-name*

Context show>router>dhcp>local-dhcp-server

Description This command displays information about declined addresses.

Parameters *ip-address* — the IP address of the DHCP server in dotted-decimal notation

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

mask — the subnet mask in Classless Inter-Domain Routing (CIDR) notation, expressed as a decimal integer

Values 0 to 32

detail — displays detailed declined address information

pool-name — the name of the DHCP IP address pool

Values up to 32 alphanumeric characters

Output The following output is an example of DHCP server declined address information, and Table 25 describes the fields.

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server local1 declined-addresses pool p1
===============================================================================
Declined addresses for server local1 3
===============================================================================
 Pool                       Subnet                IP Address
PPoe User Name/         Time                  MAC Address           Type
Option 82 Circuit ID
-------------------------------------------------------------------------------
 defaultDhcpPool           192.168.100.0/24      192.168.100.10
                          2014/01/22 21:12:55  e8:39:35:f0:cb:ed      dhcp
-------------------------------------------------------------------------------
No. of entries: 1
===============================================================================
*A:ALU-1#
```

Table 25 **DHCP Server Declined Addresses Field Descriptions**

Label	Description
Pool	The name of the DHCP address pool
PPoe User Name/Option 82 Circuit ID	The PPoE user name or Option 82 circuit ID PPoE user names are not supported on the 7705 SAR
Subnet	The subnet of the DHCP address pool
Time	The time that the address was declined
IP Address	The declined IP address
MAC Address	The declined MAC address
Type	The type of pool

free-addresses

Syntax **free-addresses** *ip-address*[*/mask*]
free-addresses summary [**subnet** *ip-address*[*/mask*]]
free-addresses pool *pool-name*

Context show>router>dhcp>local-dhcp-server

Description This command displays the free addresses in a subnet.

Parameters *ip-address* — the IP address of the DHCP server or the subnet in dotted-decimal notation

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

mask — the subnet mask in Classless Inter-Domain Routing (CIDR) notation, expressed as a decimal integer

Values 0 to 32

summary — displays summary free address information

pool-name — the name of the DHCP IP address pool

Values up to 32 alphanumeric characters

Output The following output is an example of DHCP server free address information, and Table 26 describes the fields.

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server local1 free-addresses pool p1
===============================================================================
Free addresses
===============================================================================
IP Address       Fail Ctrl
-------------------------------------------------------------------------------
10.0.0.0         local
10.0.0.1         local
10.0.0.2         local
-------------------------------------------------------------------------------
No. of free addresses: 3
===============================================================================
*A:ALU-1#
```

Table 26 **DHCP Server Free Addresses Field Descriptions**

Label	Description
IP Address	The free IP address
Fail Ctrl	The failure control Failure control is not supported on the 7705 SAR

leases

Syntax **leases** [**detail**]
leases *ip-address*[*/mask*] **address-from-user-db** [**detail**]
leases *ip-address*[*/mask*] [**detail**] [*state*]
leases *ip-address*[*/mask*] **dhcp-host** *dhcp-host-name* [**detail**]
leases [*ipv6-address*/*prefix-length*] [*type*] [*state*] [**detail**]

Context show>router>dhcp>local-dhcp-server
show>router>dhcp6>local-dhcp-server

Description This command displays DHCP or DHCPv6 lease information.

Entering the command with no parameters will show all leases.

Parameters *ip-address* — the IP address of the DHCP server in dotted-decimal notation

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

mask — the subnet mask in Classless Inter-Domain Routing (CIDR) notation, expressed as a decimal integer

Values 0 to 32

ipv6-address/prefix-length — the base IPv6 address of the subnet. This address must be unique.

Values	*ipv6-address*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d,d,d,d x: [0 to FFFF]H d: [0 to 255]D
	prefix-length	4 to 128

type — specifies the lease type to display

Values pd | slaac | wan-host

state — specifies the state of the lease to display

Values advertised | remove-pending | held | stable

detail — keyword to display detailed information of all leases in the indicated subnet

address-from-user-db — keyword to display only leases that have IP addresses from the local user database

dhcp-host-name — a DHCP host name. All leases in the local user database with a matching DHCP host are displayed.

Output The following outputs are examples of DHCP statistics information:

- DHCP lease output (Output Example, Table 27)
- DHCPv6 lease output (Output Example, Table 28)

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server local1 leases 10.0.0.0
===============================================================================
Leases for DHCP server local1 router 3
===============================================================================
IP Address       Lease State      Mac Address       Remaining       Clnt
 PPoE user name/Opt82 Circuit Id                    LifeTime        Type
 User-db-hostname
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
No leases found
===============================================================================
*A:ALU-1#
```

Table 27 **DHCP Server Lease Field Descriptions**

Label	Description
IP Address	The leased IP address
PPoE user name/Opt82 Circuit Id	The PPoE user name or Option 82 circuit ID PPoE user names are not supported on the 7705 SAR
User-db-hostname	The user database hostname User databases are not supported on the 7705 SAR
Lease State	The state of the lease. The state can be: • advertised • remove-pending • held • stable
Mac Address	The MAC address
Remaining LifeTime	The remaining time left in the lease
Clnt Type	The type of client

Output Example

```
show router 600 dhcp6 local-dhcp-server "d6" leases
===============================================================================
Leases for DHCPv6 server d6
===============================================================================
IP Address/Prefix                       Lease State      Remaining       Fail
  Link-local Address                                     LifeTime        Ctrl
-------------------------------------------------------------------------------
2001:db8::/128
  FE80::220:FCFF:FE1E:CD52              stable           23h58m52s       local
-------------------------------------------------------------------------------
1 lease found
===============================================================================
```

Table 28 **DHCPv6 Server Lease Field Descriptions**

Label	Description
IP Address/ Prefix	The leased IPv6 address and prefix
Link-local Address	The link-local address of the leased IPv6 address and prefix
Lease State	The state of the lease. The state can be: • advertised • remove-pending • held • stable
Remaining Lifetime	The amount of time remaining in the current lease
Fail Ctrl	The failure control method

pool-ext-stats

Syntax **pool-ext-stats** [*pool-name*]

Context show>router>dhcp>local-dhcp-server
show>router>dhcp6>local-dhcp-server

Description This command displays extended statistics for each DHCP or DHCPv6 pool in the local DHCP or DHCPv6 server.

For each listed statistic except for Provisioned Addresses, a current value and peak value are shown. The peak value is the highest value reached by the statistic since pool creation or the last pool statistics clearing operation via the **clear router** {**dhcp** | **dhcpv6**} **local-dhcp-server pool-ext-stats** command.

Parameters *pool-name* — the name of a DHCP or DHCPv6 pool in the local DHCP or DHCPv6 server

Output The following outputs are examples of extended DHCP or DHCPv6 pool statistics information:

- DHCP pool output (Output Example, Table 29)
- DHCPv6 pool output (Output Example, Table 30)

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server "local1" pool-ext-stats
===============================================================================
Extended pool statistics for server "local1"
===============================================================================
                          Current      Peak              TimeStamp
-------------------------------------------------------------------------------
Pool                      local1
```

```
Local:
  Stable Leases           0            0                01/07/2016 19:07:11
  Provisioned Addresses   101
  Used Addresses          0            0                01/07/2016 19:07:11
  Free Addresses          101          101              01/07/2016 19:07:11
  Used Pct                0            0                01/07/2016 19:07:11
  Free Pct                100          100              01/07/2016 19:07:11
Last Reset Time                                        01/07/2016 19:07:11
-------------------------------------------------------------------------------
Number of entries 1
===============================================================================
```

Table 29 **Extended DHCP Pool Statistics Field Descriptions**

Label	Description
Current	The current value of the statistic
Peak	The highest value reached by the statistic since pool creation or the last statistics clearing operation
TimeStamp	The date and time of the current statistic capture
Pool	The name of the pool
Offered Leases	The number of leases offered from the pool
Stable Leases	The number of stable leases in the pool
Provisioned Addresses	The number of provisioned addresses in the pool
Used Addresses	The number of used addresses in the pool
Free Addresses	The number of free addresses in the pool
Used Pct	The percentage of used addresses in the pool
Free Pct	The percentage of free addresses in the pool
Last Reset Time	The date and time of the last pool statistics clearing operation
Number of entries	The total number of pool entries

Output Example

```
show router 500 dhcp6 local-dhcp-server "d6" pool-ext-stats "pool-v6"
===============================================================================
Extended pool statistics for server "d6"
===============================================================================
                        Current       Peak           TimeStamp
-------------------------------------------------------------------------------
Pool                    pool-v6
Local:
Stable Leases           0             0              01/07/2015 19:54:52
  Provisioned Blks      4
```

```
  Used Blks              0             0             01/07/2015 19:54:52
  Free Blks              4             4             01/07/2015 19:54:52
  Used Pct               0             0             01/07/2015 19:54:52
  Free Pct               100           100           01/07/2015 19:54:52
Last Reset Time                                      01/07/2015 19:54:52
-------------------------------------------------------------------------------
Number of entries       1
===============================================================================
```

Table 30 **Extended DHCPv6 Pool Statistics Field Descriptions**

Label	Description
Current	The current value for the field
Peak	The highest value for the field since pool creation or last reset
TimeStamp	The timestamp of the current value
Pool	The name of the pool
Local	
Stable Leases	The total number of stable leases in the pool
Provisioned Blks	The number of provisioned /64 address blocks in the pool
Used Blks	The number of used /64 address blocks in the pool
Free Blks	The number of free /64 address blocks in the pool
Used Pct	The percentage of used addresses (with /64 address block)
Free Pct	The percentage of free addresses (with /64 address block)
Last Reset Time	The timestamp of the last reset
Number of entries	The total number of pool entries

pool-stats

Syntax **pool-stats** [*pool-name*]

Context show>router>dhcp6>local-dhcp-server

Description This command displays statistics per DHCPv6 pool for a local DHCPv6 server.

If no pool name is specified, statistics for all DHCPv6 pools are displayed.

Parameters *pool-name* — the name of a DHCPv6 local server pool

Output The following output is an example of DHCPv6 pool statistics, and Table 31 describes the fields.

Output Example

```
show router dhcp6 local-dhcp-server "d6" pool-stats "pool-v6"
===============================================================================
DHCPv6 server pool statistics
===============================================================================
Pool                          : pool-v6
-------------------------------------------------------------------------------
Dropped Int no prefix WAN     : 0
Dropped Int no prefix SLAAC   : 0

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

Table 31 **DHCPv6 Pool Statistics Field Descriptions**

Label	Description
Pool	The name of the pool
Dropped Int no prefix WAN	The number of routing gateway WAN interfaces dropped due to inability to provide a prefix from the pool
Dropped Int no prefix SLAAC	The number of interfaces dropped due to inability to provide a prefix from the pool using stateless address autoconfiguration

prefix-ext-stats

Syntax **prefix-ext-stats** *ipv6-address/prefix-length*
prefix-ext-stats pool *pool-name*

Context show>router>dhcp6>local-dhcp-server

Description This command displays extended statistics per DHCPv6 prefix for a local DHCPv6 server.

The current value and peak value are displayed for each statistic except for provisioned addresses. Peak value is the highest value since the prefix was created or last reset using the **clear router dhcp6 local-dhcp-server prefix-ext-stats** command.

When the **pool** parameter is used, the statistics for each prefix in the specified pool are displayed.

Parameters *ipv6-address/prefix-length* — the base IPv6 address of the local DHCPv6 server. This address must be unique.

Values *ipv6-address* x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d,d,d,d
x: [0 to FFFF]H
d: [0 to 255]D
prefix-length 4 to 128

pool-name — the name of the DHCPv6 local server pool

Output The following output is an example of extended DHCPv6 prefix statistics, and Table 32 describes the fields.

Output Example

```
show router 500 dhcp6 local-dhcp-server "d6" prefix-ext-stats 2001:db8::/62
===============================================================================
Extended statistics for prefix 2001:db8::/62
===============================================================================
                          Current       Peak           TimeStamp
-------------------------------------------------------------------------------
Local:
  Failover Oper State     Active
  Stable Leases           0             0              01/07/2015 19:54:52
  Provisioned Blks        4
  Used Blks               0             0              01/07/2015 19:54:52
  Free Blks               4             4              01/07/2015 19:54:52
  Used Pct                0             0              01/07/2015 19:54:52
  Free Pct                100           100            01/07/2015 19:54:52
Last Reset Time                                        01/07/2015 19:54:52
-------------------------------------------------------------------------------
Number of entries       1
===============================================================================
```

Table 32 **Extended DHCPv6 Prefix Statistics Field Descriptions**

Label	Description
Current	The current value for the field
Peak	The highest value for the field since pool creation or last reset
TimeStamp	The timestamp of the current value
Local	
Failover Oper State	The current state of failover capacity
Stable Leases	The total number of stable leases in the pool
Provisioned Blks	The number of provisioned /64 address blocks in the pool
Used Blks	The number of used /64 address blocks in the pool
Free Blks	The number of free /64 address blocks in the pool
Used Pct	The percentage of used addresses (with /64 address block)
Free Pct	The percentage of free addresses (with /64 address block)
Last Reset Time	The timestamp of the last reset
Number of entries	The total number of pool entries

prefix-stats

Syntax **prefix-stats** *ipv6-address/prefix-length*
prefix-stats pool *pool-name*

Context show>router>dhcp6>local-dhcp-server

Description This command displays statistics for a DHCPv6 prefix.

When the **pool** parameter is used, the statistics for each prefix in the specified pool are displayed.

Parameters *ipv6-address/prefix-length* — the base IPv6 address of the DHCPv6 prefix. This address must be unique.

Values

ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d,d,d,d x: [0 to FFFF]H d: [0 to 255]D
prefix-length	4 to 128

pool-name — the name of the DHCPv6 local server pool

Output The following output is an example of DHCPv6 prefix statistics, and Table 33 describes the fields.

Output Example

```
show router 500 dhcp6 local-dhcp-server "d6" prefix-stats 2001:db8::/62
===============================================================================
Statistics for prefix 2001:db8::/62
===============================================================
Prefix
          Advertised Stable     RCPending  RemPending Declined
---------------------------------------------------------------
2001:db8::/62
          0          0          0          0          0
---------------------------------------------------------------
Number of entries       1
===============================================================
```

Table 33 **DHCPv6 Prefix Statistics Field Descriptions**

Label	Description
Prefix	The DHCPv6 prefix
Advertised	The number of advertised leases in the prefix
Stable	The number of stable leases in the prefix

Table 33 **DHCPv6 Prefix Statistics Field Descriptions (Continued)**

Label	Description
RCPending	The number of leases in the prefix that are pending assignment based on router capability (RC) protocol
RemPending	The number of leases in the prefix that are pending removal
Declined	The number of declined leases in the prefix
Number of entries	The total number of listed prefixes

server-stats

Syntax **server-stats**

Context show>router>dhcp>local-dhcp-server
show>router>dhcp6>local-dhcp-server

Description This command displays local DHCP or DHCPv6 server statistics.

Output The following output is an example of DHCP server statistics information, and Table 34 describes the fields.

The following outputs are examples of DHCP or DHCPv6 server statistics information:

- DHCP server output (Output Example, Table 34)
- DHCPv6 server output (Output Example, Table 35)

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server local1 server-stats
===============================================================================
Statistics for DHCP Server local1 router 3
===============================================================================
Rx Discover Packets           : 1
Rx Request Packets            : 1
Rx Release Packets            : 0
Rx Decline Packets            : 0
Rx Inform Packets             : 0

Tx Offer Packets              : 1
Tx Ack Packets                : 1
Tx Nak Packets                : 0
Tx Forcerenew Packets         : 0

Client Ignored Offers         : 0
Leases Timed Out              : 0

Dropped Bad Packet            : 0
Dropped Invalid Type          : 0
Dropped No User Database      : 0
```

```
Dropped Unknown Host          : 0
Dropped User Not Allowed      : 0
Dropped Lease Not Ready       : 0
Dropped Lease Not Found       : 0
Dropped Not Serving Pool      : 0
Dropped Invalid User          : 0
Dropped Overload              : 0
Dropped Persistence Overload  : 0
Dropped Generic Error         : 0
Dropped Destined To Other     : 0
Dropped Address Unavailable   : 0
Dropped Max Leases Reached    : 0
Dropped Server Shutdown       : 0
Dropped No Subnet For Fixed IP: 0
Dropped Duplicate From Diff GI: 0
===============================================================================
```

Table 34 **DHCP Server Statistics Field Descriptions**

Label	Description
Rx Discover Packets	The number of DHCPDISCOVER (option 53 with value 1) packets received by the DHCP server
Rx Request Packets	The number of DHCPREQUEST (option 53 with value 3) packets received by the DHCP server
Rx Release Packets	The number of DHCPRELEASE (option 53 with value 7) packets received by the DHCP server
Rx Decline Packets	The number of DHCPDECLINE (option 53 with value 4) packets received by the DHCP server
Rx Inform Packets	The number of DHCPINFORM (option 53 with value 8) packets received by the DHCP server
Tx Offer Packets	The number of DHCPOFFER (option 53 with value 2) packets sent by the DHCP server
Tx Ack Packets	The number of DHCPACK (option 53 with value 5) packets sent by the DHCP server
Tx Nak Packets	The number of DHCPNAK (option 53 with value 6) packets sent by the DHCP server
Tx Forcerenew Packets	The number of DHCPFORCERENEW (option 53 with value 9) packets sent by the DHCP server
Client Ignored Offers	The number of DHCPOFFER (option 52 with value 2) packets sent by the DHCP server that were ignored by the clients
Leases Timed Out	The number of DHCP leases that timed out without renewal
Dropped Bad Packet	The number of DHCP packets received that were corrupt

Table 34 **DHCP Server Statistics Field Descriptions (Continued)**

Label	Description
Dropped Invalid Type	The number of DHCP packets received that had an invalid message type (option 53)
Dropped No User Database	The number of DHCP packets dropped because the user-db value of the server was not equal to the default value and a local user database with that name could not be found. This is not supported on the 7705 SAR.
Dropped Unknown Host	The number of DHCP packets dropped from hosts that were not found in the user database when use-gi-address was disabled
Dropped User Not Allowed	The number of DHCP packets dropped from hosts, which have no specified address or pool, that were found in the user database while use-gi-address was disabled
Dropped Lease Not Ready	The number of DHCP packets dropped by the server before the lease database was ready
Dropped Lease Not Found	The number of DHCP packets dropped by the server because no valid lease was found
Dropped Not Serving Pool	The number of DHCP packets dropped by the server because there were no free addresses in the pool
Dropped Invalid User	The number of DHCP packets dropped by the server because the MAC address of the sender or the Option 82 did not match the host lease state
Dropped Overload	The number of DHCP packets dropped by the server because they were received in excess of what the server can process
Dropped Persistence Overload	The number of DHCP packets dropped by the server because they were received in excess of what the DHCP persistence system can process. If this occurs, only releases and declines are processed.
Dropped Generic Error	The number of DHCP packets dropped by the server because of a generic error
Dropped Destined to Other	The number of DHCP requests dropped by the server because the broadcast request was not addressed to this server
Dropped Address Unavailable	The number of DHCP requests dropped by the server because the requested address is not available
Dropped Max Leases Reached	The number of DHCP packets dropped by the server because the maximum number of leases was reached
Dropped Server Shutdown	The number of DHCP packets dropped by the server during server shutdown

Table 34 **DHCP Server Statistics Field Descriptions (Continued)**

Label	Description
Dropped No Subnet For Fixed IP	The number of DHCP packets dropped by the server for user-db hosts with a fixed address because the subnet to which the address belongs is not configured
Dropped Duplicate From Diff GI	The number of DHCP requests dropped by the server because they were received from a different Gateway IP address within an interval of 10 s after the previous DHCP request

Output Example

```
*A:ALU-1# show router dhcp6 local-dhcp-server local1 server-stats
===============================================================================
Statistics for DHCP Server local1 router 3
===============================================================================
Rx Solicit Packets            : 0
Rx Request Packets            : 0
Rx Confirm Packets            : 0
Rx Renew Packets              : 0
Rx Rebind Packets             : 0
Rx Decline Packets            : 0
Rx Release Packets            : 0
Rx Information Request Packets: 0
Rx Leasequery Packets         : 0

Tx Advertise Packets          : 0
Tx Reply Packets              : 0
Tx Reconfigure Packets        : 0
Tx Leasequery Reply Packets   : 0

Client Ignored Offers         : 0
Leases Timed Out              : 0

Dropped Bad Packet            : 0
Dropped Invalid Type          : 0
Dropped Lease Not Ready       : 0
Dropped Not Serving Pool      : 0
Dropped Overload              : 0
Dropped Persistence Overload  : 0
Dropped Generic Error         : 0
Dropped Destined To Other     : 0
Dropped Max Leases Reached    : 0
Dropped Server Shutdown       : 0
Dropped Leasequery Not Allowed: 0
Dropped Duplicate             : 0
===============================================================================
*A:ALU-1#
```

Table 35 **DHCPv6 Server Statistics Field Descriptions**

Label	Description
Rx Solicit Packets	The number of SOLICIT packets received by the DHCPv6 server
Rx Request Packets	The number of REQUEST packets received by the DHCPv6 server
Rx Confirm Packets	The number of CONFIRM packets received by the DHCPv6 server
Rx Renew Packets	The number of RENEW packets received by the DHCPv6 server
Rx Rebind Packets	The number of REBIND packets received by the DHCPv6 server
Rx Decline Packets	The number of DECLINE packets received by the DHCPv6 server
Rx Release Packets	The number of RELEASE packets received by the DHCPv6 server
Rx Information Request Packets	The number of INFORMATION-REQUEST packets received by the DHCPv6 server
Rx Leasequery Packets	The number of lease query packets received by the DHCPv6 server
Tx Advertise Packets	The number of ADVERTISE packets sent by the DHCPv6 server
Tx Reply Packets	The number of REPLY packets sent by the DHCPv6 server
Tx Reconfigure Packets	The number of RECONFIGURE packets sent by the DHCPv6 server
Tx Leasequery Reply Packets	The number of REPLY packets sent by the DHCPv6 server in response to a lease query
Client Ignored Offers	The number of ADVERTISE packets sent by the DHCPv6 server that were ignored by the clients
Leases Timed Out	The number of DHCPv6 leases that timed out without renewal
Dropped Bad Packet	The number of DHCPv6 packets received that were corrupt
Dropped Invalid Type	The number of DHCPv6 packets received that had an invalid message type (option 53)
Dropped Lease Not Ready	The number of DHCPv6 packets dropped by the server before the lease database was ready
Dropped Not Serving Pool	The number of DHCPv6 packets dropped by the server because there were no free addresses in the pool

Table 35 **DHCPv6 Server Statistics Field Descriptions (Continued)**

Label	Description
Dropped Overload	The number of DHCPv6 packets dropped by the server because they were received in excess of what the server can process
Dropped Persistence Overload	The number of DHCPv6 packets dropped by the server because they were received in excess of what the DHCPv6 persistence system can process. If this occurs, only releases and declines are processed.
Dropped Generic Error	The number of DHCPv6 packets dropped by the server because of a generic error
Dropped Destined to Other	The number of DHCPv6 requests dropped by the server because the broadcast request was not addressed to this server
Dropped Max Leases Reached	The number of DHCPv6 packets dropped by the server because the maximum number of leases was reached
Dropped Server Shutdown	The number of DHCPv6 packets dropped by the server during server shutdown
Dropped Leasequery Not Allowed	The number of DHCPv6 packets dropped by the server because lease queries were disabled
Dropped Duplicate	The number of DHCPv6 requests dropped by the server because they were received from a different IP address within an interval of 10 s after the previous DHCPv6 request

subnet-ext-stats

Syntax **subnet-ext-stats** *ip-address*[/*mask*]
subnet-ext-stats pool *pool-name*

Context show>router>dhcp>local-dhcp-server

Description This command displays extended statistics for each subnet in the local DHCP server.

For each listed statistic except for Provisioned Addresses, a current value and peak value are shown. The peak value is the highest value reached by the statistic since subnet creation or the last subnet statistics clearing operation via the **clear router dhcp local-dhcp-server subnet-ext-stats** command.

Parameters *ip-address* — the IP address of the DHCP server in dotted-decimal notation

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

mask — the subnet mask in Classless Inter-Domain Routing (CIDR) notation, expressed as a decimal integer

Values 0 to 32

pool-name — the name of a DHCP pool in the local DHCP server

Output The following output is an example of extended DHCP subnet statistics, and Table 36 describes the fields.

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server "local1" subnet-ext-stats 10.10.10.0/24
===============================================================================
Extended pool statistics for subnet 10.10.10.0/24
===============================================================================
                          Current      Peak              TimeStamp
-------------------------------------------------------------------------------
Local:
  Stable Leases           1            1                 01/07/2016 19:07:11
  Provisioned Addresses   101
  Used Addresses          1            1                 01/07/2016 19:07:11
  Free Addresses          100          100               01/07/2016 19:07:11
  Used Pct                1            1                 01/07/2016 19:07:11
  Free Pct                99           99                01/07/2016 19:07:11
Last Reset Time                                         01/07/2016 19:07:11
-------------------------------------------------------------------------------
Number of entries 1
===============================================================================
```

Table 36 **Extended DHCP Subnet Statistics Field Descriptions**

Label	Description
Current	The current value of the statistic
Peak	The highest value reached by the statistic since subnet creation or the last subnet statistics clearing operation
TimeStamp	The date and time of the current statistics capture
Offered Leases	The number of leases offered from the subnet
Stable Leases	The number of stable leases in the subnet
Provisioned Addresses	The number of provisioned addresses in the subnet
Used Addresses	The number of used addresses in the subnet
Free Addresses	The number of free addresses in the subnet
Used Pct	The percentage of used addresses in the subnet
Free Pct	The percentage of free addresses in the subnet

Table 36 **Extended DHCP Subnet Statistics Field Descriptions**

Label	Description
Last Reset Time	The date and time of the last subnet statistics clearing operation
Number of entries	The total number of subnet entries

subnet-stats

Syntax **subnet-stats** *ip-address*[*/mask*]
subnet-stats pool *pool-name*

Context show>router>dhcp>local-dhcp-server

Description This command displays subnet statistics.

Parameters *ip-address* — the IP address of the DHCP server in dotted-decimal notation

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

mask — the subnet mask in Classless Inter-Domain Routing (CIDR) notation, expressed as a decimal integer

Values 0 to 32

pool-name — the name of the DHCP address pool

Values up to 32 alphanumeric characters

Output The following output is an example of DHCP server subnet statistics information, and Table 37 describes the fields.

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server local1 subnet-stats pool p1
===============================================================================
Statistics for pool p1
===============================================================================
Subnet               Free          Offered         Stable
                       FRPending     RemPending      Declined
-------------------------------------------------------------------------------
192.168.100.0/24     10            0               1
                       0             0               0
-------------------------------------------------------------------------------
No. of entries: 1
===============================================================================
*A:ALU-1#
```

Table 37 **DHCP Server Subnet Statistics Field Descriptions**

Label	Description
Subnet	The subnet of the pool
Free	The number of free leases in the subnet
FRPending	The number of leases in the subnet that are pending a force renew
Offered	The number of offered leases in the subnet
RemPending	The number of leases in the subnet that are pending removal
Stable	The number of stable leases in the subnet
Declined	The number of declined leases in the subnet

summary

Syntax **summary**

Context show>router>dhcp>local-dhcp-server
show>router>dhcp6>local-dhcp-server

Description This command displays local DHCP or DHCPv6 summary information.

Output The following outputs are examples of DHCP or DHCPv6 server summary information:

- DHCP server output (Output Example, Table 38)
- DHCPv6 server output (Output Example, Table 39)

Output Example

```
*A:ALU-1# show router dhcp local-dhcp-server local1 summary
===============================================================================
DHCP server local1 router 3
===============================================================================
local1-p1
Admin State            : inService
Persistency State      : ok
User Data Base         : N/A
Use gateway IP address : enabled
Send force-renewals    : disabled

-------------------------------------------------------------------------------
Pool name : p1
-------------------------------------------------------------------------------
Subnet            Free         Stable    Declined   Offered    Remove-pending
-------------------------------------------------------------------------------
10.0.0.0/8         16384        0         0          0          0
```

```
Totals for pool   16384        0         0          0          0
-------------------------------------------------------------------------------
Totals for server 16384        0         0          0          0
-------------------------------------------------------------------------------
Associations                    Admin
-------------------------------------------------------------------------------
No associations found
===============================================================================
*A:ALU-1#
```

Table 38 DHCP Server Summary Field Descriptions

Label	Description
Admin State	The administrative state of the DHCP server
Persistency State	The persistence state of the DHCP server
User Data Base	Indicates whether the DHCP server uses a user database
Use gateway IP address	Indicates whether the DHCP server uses GIADDR
Send force-renewals	Indicates whether the DHCP server sends FORCERENEW messages
Pool	
Subnet	The subnet of the pool
Free	The number of free IP addresses in the subnet
Stable	The number of stable IP addresses in the subnet
Declined	The number of declined IP addresses in the subnet
Offered	The number of offered IP addresses in the subnet
Remove-pending	The number of IP addresses pending removal in the subnet
Associations	
Associations	The name of the associated interface
Admin	The administrative state of the interface

Output Example

```
*A:ALU-1# show router dhcp6 local-dhcp-server local1 summary
===============================================================================
DHCP server local1 router 3
===============================================================================
Admin State             : inService
Operational State       : inService
Persistency State       : ok
Use Link Address        : enabled (scope subject)
```

```
Use pool from client   : disabled
Creation Origin        : manual
Lease Hold Time        : 0h0m0s
Lease Hold Time For    : N/A
User-ident             : duid
Interface-id-mapping   : disabled
Ignore-rapid-commit    : disabled
Allow-lease-query      : disabled
User Data Base         : N/A

-------------------------------------------------------------------------------
Pool name : p1
-------------------------------------------------------------------------------
Subnet            Free         Stable    Declined   Offered    Remove-pending
-------------------------------------------------------------------------------
10.0.0.0/8         16384        0         0          0          0

Totals for pool   16384        0         0          0          0
-------------------------------------------------------------------------------
Totals for server 16384        0         0          0          0
-------------------------------------------------------------------------------
Associations                    Admin
-------------------------------------------------------------------------------
No associations found
===============================================================================
*A:ALU-1#
```

Table 39 **DHCPv6 Server Summary Field Descriptions**

Label	Description
Admin State	The administrative state of the DHCPv6 server
Operational State	The operational state of the DHCPv6 server
Persistency State	The persistence state of the DHCPv6 server
Use Link Address	Indicates whether **use-link-address** is enabled, and, if enabled, the scope
Use pool from client	Indicates whether **use-pool-from-client** is enabled
Creation Origin	The creation method of the DHCPv6 server
Lease Hold Time	The lease retention time configured using the **lease-hold-time** command
Lease Hold Time For	The lease being held by the DHCPv6 server
User-ident	The user identification method configured using the **user-ident** command
Interface-id-mapping	Indicates whether interface ID mapping is enabled
Ignore-rapid-commit	Indicates whether the DHCPv6 server is configured to ignore rapid committing

Table 39 **DHCPv6 Server Summary Field Descriptions (Continued)**

Label	Description
Allow-lease-query	Indicates whether the DHCPv6 server allows lease query messages
Pool	
Subnet	The subnet of the pool
Free	The number of free IP addresses in the subnet
Stable	The number of stable IP addresses in the subnet
Declined	The number of declined IP addresses in the subnet
Offered	The number of offered IP addresses in the subnet
Remove-pending	The number of IP addresses pending removal in the subnet
Associations	
Associations	The name of the associated interface
Admin	The administrative state of the interface

servers

Syntax **servers** [**all**]

Context show>router>dhcp
show>router>dhcp6

Description This command lists the local DHCP or DHCPv6 servers.

Parameters **all** — displays DHCP or DHCPv6 servers in all instances

Output The following output is an example of DHCP server information, and Table 40 describes the fields.

Output Example

```
*A:ALU-1# show router dhcp servers
===============================================================================
Overview of DHCP Servers
===============================================================================
Active Leases:      1
Maximum Leases:     4096

Router              Server                                  Admin State
-------------------------------------------------------------------------------
Router: Base        dhcpServer1                             inService
Service: 102        vprnServer                              inService
```

Table 40 **DHCP or DHCPv6 Server Field Descriptions**

Label	Description
Active Leases	The number of active leases
Maximum Leases	The maximum number of leases available
Router	The name of the router
Server	The name of the DHCP or DHCPv6 server
Admin State	The administrative state of the DHCP or DHCPv6 server

statistics

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

Context show>router>dhcp
show>router>dhcp6

Description This command displays statistics for DHCP Relay and DHCPv6 Relay.

If no interface name or IP address is specified, then all configured interfaces are displayed. If the **statistics** command is used in the **dhcp6** context, the interface name or IP address cannot be specified.

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

Output The following outputs are examples of DHCP or DHCPv6 statistics information:

- DHCP statistics (Output Example, Table 41)
- DHCPv6 statistics (Output Example, Table 42)

Output Example

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

Table 41 **DHCP Statistics Field Descriptions**

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

Output Example

```
*A:ALU-1# show router dhcp6 statistics
===============================================================================
DHCP6 statistics (Router: Base)
===============================================================================
Msg-type                        Rx              Tx              Dropped
-------------------------------------------------------------------------------
1 SOLICIT                       0               0               0
2 ADVERTISE                     0               0               0
3 REQUEST                       0               0               0
4 CONFIRM                       0               0               0
5 RENEW                         0               0               0
6 REBIND                        0               0               0
7 REPLY                         0               0               0
8 RELEASE                       0               0               0
9 DECLINE                       0               0               0
10 RECONFIGURE                  0               0               0
11 INFO_REQUEST                 0               0               0
12 RELAY_FORW                   0               0               0
13 RELAY_REPLY                  0               0               0

-------------------------------------------------------------------------------
Dhcp6 Drop Reason Counters :
-------------------------------------------------------------------------------
 1 Dhcp6 oper state is not Up on src itf                          0
 2 Dhcp6 oper state is not Up on dst itf                          0
 3 Relay Reply Msg on Client Itf                                  0
 4 Hop Count Limit reached                                        0
 5 Missing Relay Msg option, or illegal msg type                  0
```

```
 6 Unable to determine destination client Itf                    0
 7 Out of Memory                                                 0
 8 No global Pfx on Client Itf                                   0
 9 Unable to determine src Ip Addr                               0
10 No route to server                                            0
11 Subscr. Mgmt. Update failed                                   0
12 Received Relay Forw Message                                   0
13 Packet too small to contain valid dhcp6 msg                   0
14 Server cannot respond to this message                         0
15 No Server Id option in msg from server                        0
16 Missing or illegal Client Id option in client msg             0
17 Server Id option in client msg                                0
18 Server DUID in client msg does not match our own              0
19 Client sent message to unicast while not allowed              0
20 Client sent message with illegal src Ip address               0
21 Client message type not supported in pfx delegation           0
22 Nbr of addrs or pfxs exceeds allowed max (128) in msg         0
23 Unable to resolve client's mac address                        0
24 The Client was assigned an illegal address                    0
25 Illegal msg encoding                                          0
===============================================================================
*A:ALU-1#
```

Table 42 **DHCPv6 Statistics Field Descriptions**

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

summary

Syntax **summary**

Context show>router>dhcp
show>router>dhcp6

Description This command displays a summary of DHCP and DHCPv6 configuration.

Output The following outputs are examples of DHCP or DHCPv6 summary information:

- DHCP summary (Output Example, Table 43)
- DHCPv6 summary (Output Example, Table 44)

Output Example

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

Table 43 **DHCP Summary Field Descriptions**

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

Output Example

```
*A:ALU-48# show router dhcp6 summary
===============================================================================
DHCP6 Summary (Router: Base)
===============================================================================
Interface Name                   Nbr      Used/Max Relay     Admin  Oper Relay
  SapId                          Resol.   Used/Max Server    Admin  Oper Server
```

```
-------------------------------------------------------------------------------
iesSap                          No          0/0             Down    Down
  sap:1/2/3:801                             0/8000          Down    Down
iesintf                         No          0/0             Down    Down
  sdp:spoke-5:9999                          0/8000          Down    Down
-------------------------------------------------------------------------------
Interfaces: 2
===============================================================================
*A:ALU-48#
```

Table 44 **DHCPv6 Summary Field Descriptions**

Label	Description
DHCP Summary (Router: Base)	
Interface Name SapId	The name of the interface or SAP/SDP identifier
Nbr Resol.	Yes — neighbor resolution (discovery) is enabled
	No — neighbor resolution (discovery) is disabled
Used/Max Relay:	Used — number of relay routes currently being used on the interface
	Max Relay — maximum number of relay routes on the interface
Used/Max Server	Used — number of server routes currently being used on the interface
	Max Server — maximum number of server routes currently being used on the interface
Admin	The administrative state
Oper Relay	The operating state of the relay routes
Oper Server	The operating state of the server routes
Interfaces	The total number of DHCPv6 interfaces

ecmp

Syntax **ecmp**

Context show>router

Description This command displays the ECMP settings for the router.

Output The following output is an example of router ECMP information, and Table 45 describes the fields.

Output Example

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

Table 45 **ECMP Settings Field Descriptions**

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

fib

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

Context show>router

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

The following adapter cards and platforms support the full IPv6 subnet range for IPv6 static routes:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card, version 2 and version 3
- 2-port 10GigE (Ethernet) Adapter card (on the v-port)
- 10-port 1GigE/1-port 10GigE X-Adapter card
- 7705 SAR-X

For these cards and platforms, the supported route range for statically provisioned or dynamically learned routes is from /1 to /128.

For all other cards, modules, and ports (including the v-port on the 2-port 10GigE (Ethernet) module), the supported range for statically provisioned or dynamically learned routes is from /1 to /64 or is /128 (indicating a host route).

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

Values 1

family — displays the router IP interface table

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

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

Values	*ipv4-prefix*	a.b.c.d (host bits must be 0)
	ipv4-prefix-length	0 to 32
Values	*ipv6-prefix*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	ipv6-prefix-length	{0 to 128} | {0 to 64 | 128}

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

secondary — displays secondary FIB information

extensive — displays next-hop FIB information

all — displays all FIB information for the specified slot number

summary — displays summary FIB information for the specified slot number

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

Output The following outputs are examples of FIB information, and Table 46 describes the fields.

Output Example

```
*A:Sar18 Dut-B>show>router# fib 1
===============================================================================
FIB Display
===============================================================================
Prefix [Flags]                                                  Protocol
  NextHop
-------------------------------------------------------------------------------
1.1.1.1/32                                                      STATIC
  10.1.1.1 (toA)
2.2.2.2/32                                                      LOCAL
  2.2.2.2 (system)
10.1.1.0/24                                                     LOCAL
  10.1.1.0 (toA)
-------------------------------------------------------------------------------
```

```
Total Entries : 3
------------------------------------------------------------------------------
==============================================================================
*A:Sar18 Dut-B>show>router#

*A:7705:Dut-C# show router fib 1 summary
==============================================================================
FIB Summary
==============================================================================
                              Active
------------------------------------------------------------------------------
Static                        0
Direct                        0
HOST                          0
BGP                           0
BGP VPN                       0
BGP LABEL                     0
OSPF                          0
ISIS                          0
RIP                           0
LDP                           0
Aggregate                     0
Sub Mgmt                      0
VPN Leak                      0
TMS                           0
Managed                       0
------------------------------------------------------------------------------
Total Installed               0
------------------------------------------------------------------------------
Current Occupancy             0%
Overflow Count                0
Suppressed by Selective FIB   0
Occupancy Threshold Alerts
    Alert Raised 0 Times;
==============================================================================
*A:7705:Dut-C#

*A:7705:Dut-C# show router 1 fib 1 extensive
==============================================================================
FIB Display (Service: 1)
==============================================================================
Dest Prefix             : 10.1.13.0/24
  Protocol              : BGP_VPN
  Installed             : Y
  Indirect Next-Hop     : 10.20.1.1
    Label               : 131070
    QoS                 : Priority=n/c, FC=n/c
    Source-Class        : 0
    Dest-Class          : 0
    ECMP-Weight         : 1
    Resolving Next-Hop  : 10.20.1.1 (RSVP tunnel:1)
      ECMP-Weight       : 1
------------------------------------------------------------------------------
Dest Prefix             : 10.1.14.0/24
  Protocol              : BGP_VPN
  Installed             : Y
  Indirect Next-Hop     : 10.20.1.2
    Label               : 131070
```

```
    QoS                 : Priority=n/c, FC=n/c
    Source-Class        : 0
    Dest-Class          : 0
    ECMP-Weight         : 1
    Resolving Next-Hop  : 10.20.1.2 (RSVP tunnel:2)
      ECMP-Weight       : 1
-------------------------------------------------------------------------------
Dest Prefix             : 10.1.15.0/24
  Protocol              : LOCAL
  Installed             : Y
  Next-Hop              : N/A
    Interface           : ies-1-10.1.15.3 (VPRN 1)
    QoS                 : Priority=n/c, FC=n/c
    Source-Class        : 0
    Dest-Class          : 0
    ECMP-Weight         : 1
-------------------------------------------------------------------------------
Dest Prefix             : 10.1.16.0/24
  Protocol              : BGP_VPN
  Installed             : Y
  Indirect Next-Hop     : 10.20.1.4
    Label               : 131070
    QoS                 : Priority=n/c, FC=n/c
    Source-Class        : 0
    Dest-Class          : 0
    ECMP-Weight         : 1
    Resolving Next-Hop  : 10.20.1.4 (RSVP tunnel:3)
      ECMP-Weight       : 1
-------------------------------------------------------------------------------
Dest Prefix             : 10.1.13.1/32
  Protocol              : BGP_VPN
  Installed             : Y
  Indirect Next-Hop     : 10.20.1.1
    Label               : 131070
    QoS                 : Priority=n/c, FC=n/c
    Source-Class        : 0
    Dest-Class          : 0
    ECMP-Weight         : 1
    Resolving Next-Hop  : 10.20.1.1 (RSVP tunnel:1)
      ECMP-Weight       : 1
-------------------------------------------------------------------------------
<snip>
*A:7705:Dut-C#

*A:7705:Dut-C# show router fib all summary
===============================================================================
FIB Slot Summary
===============================================================================
Slot                Occupancy           Installed           Suppressed by FIB
-------------------------------------------------------------------------------
1                   1%                  2                   0
===============================================================================
```

Table 46 **FIB Field Descriptions**

Label	Description
Active	The number of active entries in the FIB for each type of route
Total Installed	The total number of active entries in the FIB
Current Occupancy	The percentage of the FIB that is being used; an alert is raised when the percentage exceeds 70% and a clear event is raised when the percentage drops below 65%
Overflow Count	The number of times that the FIB was full
Suppressed by Selective FIB	The number of entries suppressed by the FIB
Occupancy Threshold Alerts	The number of times a threshold alert was raised to indicate that more than 70% of the FIB is being used
Prefix[Flags] Dest Prefix	The route destination address and mask
Protocol	The active protocol (LOCAL, STATIC, OSPF, ISIS, AGGREGATE, BGP, RIP, or BGP-VPN)
Installed	Indicates whether the route is installed in the FIB
Next Hop or Indirect Next-Hop	The next-hop or indirect next-hop IP address for the route destination
Interface	The interface name of the next hop
QoS	The FC and priority associated with the next hop
Source-Class	The source class value, 0 to 255
Dest-Class	The destination class value, 0 to 255
ECMP-Weight	The fractional share of bandwidth for the next hop, indirect next hop, or resolving next hop, either N/A or 1 to 32
Total Entries	The total number of next-hop entries

icmp

Syntax **icmp**

Context show>router

Description This command displays ICMP statistics. ICMP generates error messages to report errors during processing and other diagnostic functions.

Output The following output is an example of ICMP information, and Table 47 describes the fields.

Output Example

```
*A:7705:Dut-A# show router icmp
===============================================================================
Global ICMP Stats
===============================================================================
Received
Total                    : 1             Error                  : 1
Destination Unreachable  : 1             Redirect               : 0
Echo Request             : 0             Echo Reply             : 0
TTL Expired              : 0             Source Quench          : 0
Timestamp Request        : 0             Timestamp Reply        : 0
Address Mask Request     : 0             Address Mask Reply     : 0
Parameter Problem        : 0
-------------------------------------------------------------------------------
Sent
Total                    : 0             Error                  : 0
Destination Unreachable  : 0             Redirect               : 0
Echo Request             : 0             Echo Reply             : 0
TTL Expired              : 0             Source Quench          : 0
Timestamp Request        : 0             Timestamp Reply        : 0
Address Mask Request     : 0             Address Mask Reply     : 0
Parameter Problem        : 0
===============================================================================
```

Table 47 ICMP Field Descriptions

Label	Description
Total	The total number of ICMP messages received or sent
Error	The total number of ICMP messages classified as errors that were received or sent
Destination Unreachable	The total number of destination unreachable messages received or sent
Redirect	The total number of redirects received or sent
Echo Request	The total number of echo requests received or sent
Echo Reply	The total number of echo replies received or sent
TTL Expired	The total number of TTL expiry messages received or sent
Source Quench	The total number of source quench messages received or sent
Timestamp Request	The total number of timestamp requests received or sent
Timestamp Reply	The total number of timestamp replies received or sent
Address Mask Request	The total number of address mask requests received or sent

Table 47 **ICMP Field Descriptions (Continued)**

Label	Description
Address Mask Reply	The total number of address mask replies received or sent
Parameter Problem	The total number of parameter problem messages received or sent

icmp6

Syntax **icmp6**

Context show>router

Description This command displays ICMPv6 statistics. ICMPv6 generates error messages to report errors during processing and other diagnostic functions. ICMPv6 packets can be used in the neighbor discovery protocol.

Output The following output is an example of ICMPv6 information, and Table 48 describes the fields.

Output Example

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

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

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

Table 48 **ICMPv6 Field Descriptions**

Label	Description
Total	The total number of ICMPv6 messages received or sent
Errors	The number of ICMPv6 messages classified as errors received or sent
Destination Unreachable	The number of destination unreachable messages received or sent
Redirects	The number of redirect messages received or sent
Time Exceeded	The number of time exceeded messages received or sent
Pkt Too Big	The number of packet-too-big messages received or sent
Echo Request	The number of echo request messages received or sent
Echo Reply	The number of echo reply messages received or sent
Router Solicits	The number of router solicit messages received or sent
Router Advertisements	The number of router advertisement messages received or sent
Neighbor Solicits	The number of neighbor solicit messages received or sent
Neighbor Advertisements	The number of neighbor advertisement messages received or sent

interface

Syntax **interface** [*interface-name*]

Context show>router>icmp
show>router>icmp6

Description This command displays ICMP or ICMPv6 statistics for all interfaces or for a specified interface. Specifying an interface name displays the ICMP or ICMPv6 information associated with that interface.

Parameters *interface-name* — specifies an existing IP interface, up to 32 characters

Output The following output is an example of ICMP interface information, and Table 49 describes the fields.

Output Example

```
*A:7705:Dut-A# show router icmp interface "nodeAC"
===============================================================================
Interface ICMP Stats
===============================================================================
===============================================================================
Interface "nodeAC"
-------------------------------------------------------------------------------
Received
Total                    : 0            Error                  : 0
Destination Unreachable  : 0            Redirect               : 0
Echo Request             : 0            Echo Reply             : 0
TTL Expired              : 0            Source Quench          : 0
Timestamp Request        : 0            Timestamp Reply        : 0
Address Mask Request     : 0            Address Mask Reply     : 0
Parameter Problem        : 0
-------------------------------------------------------------------------------
Sent
Total                    : 0            Error                  : 0
Destination Unreachable  : 0            Redirect               : 0
Echo Request             : 0            Echo Reply             : 0
TTL Expired              : 0            Source Quench          : 0
Timestamp Request        : 0            Timestamp Reply        : 0
Address Mask Request     : 0            Address Mask Reply     : 0
Parameter Problem        : 0
===============================================================================
```

Table 49 ICMP Interface Field Descriptions

Label	Description
Total	The total number of ICMP messages received or sent
Error	The total number of ICMP messages classified as errors that are received or sent
Destination Unreachable	The total number of destination unreachable messages received or sent
Redirect	The total number of redirects received or sent
Echo Request	The total number of echo requests received or sent
Echo Reply	The number of echo replies received or sent
TTL Expired	The total number of TTL expiry messages received or sent
Source Quench	The total number of source quench messages received or sent
Timestamp Request	The total number of timestamp requests received or sent
Timestamp Reply	The total number of timestamp replies received or sent
Address Mask Request	The total number of address mask requests received or sent

Table 49 **ICMP Interface Field Descriptions (Continued)**

Label	Description
Address Mask Reply	The total number of address mask replies received or sent
Parameter Problem	The total number of parameter problem messages received or sent

The following output is an example of ICMPv6 interface information, and Table 50 describes the fields.

Output Example

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

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

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

Table 50 **ICMPv6 Interface Field Descriptions**

Label	Description
Total	The total number of all ICMPv6 messages received or sent
Errors	The number of ICMPv6 messages classified as errors received or sent
Destination Unreachable	The number of destination unreachable messages received or sent
Redirects	The number of redirect messages received or sent

Table 50 **ICMPv6 Interface Field Descriptions (Continued)**

Label	Description
Time Exceeded	The number of time exceeded messages received or sent
Pkt Too Big	The number of packet-too-big messages received or sent
Echo Request	The number of echo request messages received or sent
Echo Reply	The number of echo reply messages received or sent
Router Solicits	The number of router solicit messages received or sent
Router Advertisements	The number of router advertisement messages received or sent
Neighbor Solicits	The number of neighbor solicit messages received or sent
Neighbor Advertisements	The number of neighbor advertisement messages received or sent

interface

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

Context show>router

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

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

Values *ipv4-address* a.b.c.d
ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

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

detail — displays detailed IP interface information

family — displays the specified router IP interface family

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

summary — displays summary IP interface information

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

statistics — displays the number of transmitted, received, and discarded packets and bytes at the Layer 3 level for IP interface statistics. The collection of IP interface statistics is supported on any IP interface, regardless of encapsulation. Supported IP interfaces are access (IES, VPRN, routed VPLS, and spoke SDP) and network (IPv4, IPv6, and MPLS) interfaces. Discard statistics are only displayed for IPv4 interfaces.

security — displays NAT and firewall session security statistics for the specified interface

tcp-mss — displays TCP MSS information for the specified interface

Output The following outputs are examples of IP interface information:

- standard IP interface information (Output Example (standard), Table 51)
- summary IP interface information (Output Example (summary), Table 52)
- detailed IP interface information (Output Example (detail), Table 53)
- statistics IP interface information (Output Example (statistics), Table 53)
- security IP interface information (Output Example (security), Table 53)
- TCP MSS information (Output Example (tcp-mss), Table 54)

Output Example (standard)

```
*A:ALU-1# show router interface
===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name                   Adm         Opr(v4/v6)  Mode    Port/SapId
   IP-Address                                                    PfxState
-------------------------------------------------------------------------------
ip-10.0.0.2                     Up          Down/Down   Network 1/1/1
   10.10.0.2/10                                                  n/a
system                           Up          Down/Down   Network system
   -                                                             -
to-103                           Up          Down/Down   Network n/a
   -                                                             -
-------------------------------------------------------------------------------
Interfaces : 3
===============================================================================

*A:ALU-1# show router interface to-103
===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name                   Adm         Opr (v4/v6)      Mode    Port/SapId
   IP-Address                                                    PfxState
-------------------------------------------------------------------------------
to-103                           Up          Down/Down        Network n/a
   -                                                             -
-------------------------------------------------------------------------------
```

Table 51 **Standard IP Interface Field Descriptions**

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

Output Example (summary)

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

Table 52 **Summary IP Interfaces Field Descriptions**

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

Output Example (detail)

```
*A:ALU-1# show router interface shaped_if_example detail
===============================================================================
Interface Table (Router: Base)
===============================================================================
-------------------------------------------------------------------------------
Interface
-------------------------------------------------------------------------------
If Name          : shaped_if_example
Admin State      : Up                    Oper (v4/v6)      : Down/Down
Protocols        : None
IP Addr/mask     : 10.10.10.1/24         Address Type      : Primary
IGP Inhibit      : Disabled              Broadcast Address : Host-ones
IPv6 Address     : 2001:1234:5678:abcd:1234:5678:1234:5678/64
IPv6 Addr State  : INACCESSIBLE
Link Lcl Address : fe80::36aa:99ff:feef:1643/64
Link Lcl State   : INACCESSIBLE
-------------------------------------------------------------------------------
Details
-------------------------------------------------------------------------------
Description      : (Not Specified)
If Index         : 21                    Virt. If Index    : 21
Last Oper Chg    : 07/11/2014 14:59:42   Global If Index   : 108
Port Id          : 1/10/5:55
TOS Marking      : Trusted               If Type           : Network
Egress Filter    : none                  Ingress Filter    : none
Egr IPv6 Flt     : none                  Ingr IPv6 Flt     : none
SNTP B.Cast      : False                 QoS Policy        : 1
Queue-group      : None
MAC Address      :                       Arp Timeout       : 14400
TCP MSS V4       : 5000                  TCP MSS V6        : 4000
IP Oper MTU      : 1554                  ICMP Mask Reply   : True
Arp Populate     : Disabled
LdpSyncTimer     : None                  Strip-Label       : Disabled
LSR Load Balance : system
TEID Load Balance: Disabled
L4 Load Balance  : system
Reassem. Profile : 16
uRPF Chk         : disabled
uRPF Fail Bytes  : 0                     uRPF Chk Fail Pkts: 0
Rx Pkts          : 0                     Rx Bytes          : 0
Rx V4 Pkts       : 0                     Rx V4 Bytes       : 0
Rx V4 Discard Pk*: 0                     Rx V4 Discard Byt*: 0
 Inv Hdr CRC Pkts: 0                      Inv Hdr CRC Bytes: 0
 Inv Length Pkts : 0                      Inv Length Bytes : 0
 Inv GRE Protoco*: 0                      Inv GRE Protocol*: 0
 Dest Unreach Pk*: 0                      Dest Unreach Byt*: 0
 Inv Mcast Addr *: 0                      Inv Mcast Addr B*: 0
 Directed Bcast *: 0                      Directed Bcast B*: 0
 Src Martian Add*: 0                      Src Martian Addr*: 0
 Dest Martian Ad*: 0                      Dest Martian Add*: 0
 Black Hole Pkts : 0                      Black Hole Bytes : 0
 FltrActionDrop *: 0                      FltrActionDrop B*: 0
 FltrNHUnreach P*: 0                      FltrNHUnreach By*: 0
 FltrNHNotDirect*: 0                      FltrNHNotDirect *: 0
 TTL Expired Pkts: 0                      TTL Expired Bytes: 0
 Slowpath Pkts   : 0                      Slowpath Bytes   : 0
 MTU Exceeded Pk*: 0                      MTU Exceeded Byt*: 0
```

```
 Queue Pkts      : 0                    Queue Bytes      : 0
 EncryptionDrop *: 0                    EncryptionDrop B*: 0
  Last Tunnel    : (Not Specified)
 Other Discards *: 0                    Other Discards B*: 0
Rx V6 Pkts       : 0                   Rx V6 Bytes       : 0
Rx V6 Discard Pk*: 0                   Rx V6 Discard Byt*: 0
 Inv Length Pkts : 0                    Inv Length Bytes : 0
 Dest Unreach Pk*: 0                    Dest Unreach Byt*: 0
 Inv Mcast Addr *: 0                    Inv Mcast Addr B*: 0
 Src Martian Add*: 0                    Src Martian Addr*: 0
 Dest Martian Ad*: 0                    Dest Martian Add*: 0
 Black Hole Pkts : 0                    Black Hole Bytes : 0
 FltrActionDrop *: 0                    FltrActionDrop B*: 0
 TTL Expired Pkts: 0                    TTL Expired Bytes: 0
 Slowpath Pkts   : 0                    Slowpath Bytes   : 0
 MTU Exceeded Pk*: 0                    MTU Exceeded Byt*: 0
 Queue Pkts      : 0                    Queue Bytes      : 0
 Other Discards *: 0                    Other Discards B*: 0
Tx V4 Pkts       : 0                   Tx V4 Bytes       : 0
Tx V4 Discard Pk*: 0                   Tx V4 Discard Byt*: 0
 FltrActionDrop *: 0                    FltrActionDrop B*: 0
 EncryptionDrop *: 0                    EncryptionDrop B*: 0
  Last Tunnel    : (Not Specified)
 Other Discards *: 0                    Other Discards B*: 0
Tx V6 Pkts       : 0                   Tx V6 Bytes       : 0
Tx V6 Discard Pk*: 0                   Tx V6 Discard Byt*: 0
 FltrActionDrop *: 0                    FltrActionDrop B*: 0
 Other Discards *: 0                    Other Discards B*: 0
Security Details
Admin Zone       : None                Oper Zone         : None
Bypass           : No
Rx V4 Discard Pk*: 0                   Rx V4 Discard Byt*: 0
 Unsup Proto Pkts: 0                    Unsup Proto Bytes: 0
 Unsup Svc Pkts  : 0                    Unsup Svc Bytes  : 0
 Unsup ICMP Type*: 0                    Unsup ICMP Type *: 0
 Fragment Pkts   : 0                    Fragment Bytes   : 0
 No Session Pkts : 0                    No Session Bytes : 0
 NAT Rte Loop Pk*: 0                    NAT Rte Loop Byt*: 0
 Other Discards *: 0                    Other Discards B*: 0
-------------------------------------------------------------------------------
IPV4 GRE Fragmentation & Reassembly Statistics
-------------------------------------------------------------------------------
Frag Tx Pkts     : 500                 Frag TX Bytes     : 121000
Frag Rx Pkts     : 250500              Frag Rx Bytes     : 60621000
Frag Rx Drp Pkts : 0                   Frag Rx Drp Bytes : 0
ExpiredWait Count: 0
-------------------------------------------------------------------------------
Proxy ARP Details
-------------------------------------------------------------------------------
Rem Proxy ARP    : Disabled            Local Proxy ARP   : Disabled
Policies         : none

Proxy Neighbor Discovery Details
Local Pxy ND     : Disabled
Policies         : none

DHCP no local server

DHCP Details
```

```
Description  : (Not Specified)
Admin State      : Down
Action           : Keep                 Copy To Opt43     : Disabled

ICMP Details
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 Addr: Not configured
Peer Sec DNS Addr: Not configured

DHCP CLIENT Details
DHCP Client     :Disabled
client-id: n/a
vendor-id: n/a

Network Domains Associated
default

-------------------------------------------------------------------------------
Admin Groups
-------------------------------------------------------------------------------
"group 1"                          "group 2"
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Srlg Groups
-------------------------------------------------------------------------------
"group 3"                          "group 4"
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Qos Details
-------------------------------------------------------------------------------
Egr Queue Pol    : policy_8
Egr Agg RateLimit: max
Egr Agg Cir      : 0 Kbps
-------------------------------------------------------------------------------
Queue Statistics
-------------------------------------------------------------------------------
Egress Queue  1              Packets                 Octets
     In Profile  forwarded :    0                       0
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0
Egress Queue  2              Packets                 Octets
     In Profile  forwarded :    0                       0
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0
Egress Queue  3              Packets                 Octets
     In Profile  forwarded :    0                       0
     In Profile  dropped   :    0                       0
     Out Profile forwarded :    0                       0
     Out Profile dropped   :    0                       0
-------------------------------------------------------------------------------
===============================================================================
```

Table 53 **Detailed IP Interface Field Descriptions**

Label	Description
Interface	
If Name	The IP interface name
Admin State	Down — the IP interface is administratively disabled
	Up — the IP interface is administratively enabled
Oper State	Down — the IP interface is operationally disabled
	Up — the IP interface is operationally enabled
Protocols	The protocol type running on the interface
IP Addr/mask	The IPv4 address and subnet mask length of the IPv4 interface n/a — no IP address has been assigned to the IPv4 interface
Address Type	This is always “Primary” on a network interface
IGP Inhibit	This is always “Disabled” on a network interface
IPv6 Address	The address and prefix length of the IPv6 interface
IPv6 Addr State	The IPv6 address state Possible states are: • PREFERRED (valid, can be used as the destination or source address) • DEPRECATED (valid but should no longer be used) • INVALID (not valid, should not be used) • INACCESSIBLE (not accessible because the interface to which this address is assigned is not operational) • UNKNOWN (the status cannot be determined, should not be used) • TENTATIVE (the uniqueness is being verified, should not be used for general communication) • DUPLICATE (non-unique, must not be used)
Link Lcl Address	The link-local address of the IPv6 interface

Table 53 **Detailed IP Interface Field Descriptions (Continued)**

Label	Description
Link Lcl State	The IPv6 link-local address state Possible states are: • PREFERRED (valid, can be used as the destination or source address) • DEPRECATED (valid but should no longer be used) • INVALID (not valid, should not be used) • INACCESSIBLE (not accessible because the interface to which this address is assigned is not operational) • UNKNOWN (the status cannot be determined, should not be used) • TENTATIVE (the uniqueness is being verified, should not be used for general communication) • DUPLICATE (non-unique, must not be used)
Broadcast Address	This is always “Host-ones” on a network interface
Details	
If Index	The interface index of the IP router interface
Virt If Index	The virtual interface index of the IP router interface
Last Oper Chg	The last change in operational status
Global If Index	The global interface index of the IP router interface
Port ID	The port identifier
TOS Marking	The ToS byte value in the logged packet
If Type	Network — the IP interface is a network/core IP interface
Egress Filter	Indicates whether an egress IPv4 filter is applied to the interface
Ingress Filter	Indicates whether an ingress IPv4 filter is applied to the interface
Egr IPv6 Flt	Indicates whether an egress IPv6 filter is applied to the interface
Ingr IPv6 Flt	Indicates whether an ingress IPv6 filter is applied to the interface
SNTP B.Cast	False — the IP interface will not send SNTP broadcast messages
	True — the IP interface will send SNTP broadcast messages
QoS Policy	Indicates the QoS policy applied to the interface
Queue-group	n/a
MAC Address	The MAC address of the IP interface

Table 53 **Detailed IP Interface Field Descriptions (Continued)**

Label	Description
TCP MSS V4	The TCP maximum segment size (MSS) configured for TCP packets on an IPv4 interface
TCP MSS V6	The TCP maximum segment size (MSS) configured for TCP packets on an IPv6 interface
Arp Timeout	The ARP timeout for the interface, in seconds, which is the time that an ARP entry is maintained in the ARP cache without being refreshed
IP Oper MTU	The operational IP Maximum Transmission Unit (MTU) for the IP interface
ICMP Mask Reply	False — the IP interface will not reply to a received ICMP mask request
	True — the IP interface will reply to a received ICMP mask request
Arp Populate	Displays if ARP is enabled or disabled
LdpSyncTimer	Specifies the IGP/LDP sync timer value
Strip-Label	Indicates that the strip label is enabled or disabled
LSR Load Balance	Indicates the LSR load balance
TEID Load Balance	Indicates whether the tunnel endpoint ID (TEID) load balance is enabled or disabled
L4 Load Balance	Indicates the L4 load balance
Reassem. Profile	The reassembly profile ID
uRPF Chk	Indicates whether unicast reverse path forwarding (uRPF) checking is enabled or disabled on this interface
uRPF Fail Bytes	The number of uRPF failures, in bytes
uRPF Chk Fail Pkts	The number of uRPF checking failures, in packets
Rx Pkts Rx Bytes	The total number of IPv4 and IPv6 packets or bytes received on the interface. This output field may display N/A for spoke SDP and IES interfaces due to MPLS packets not contributing to this statistics counter.
Rx V4 Pkts Rx V4 Bytes	The number of IPv4 packets or bytes received on the interface. This output field may display N/A for spoke SDP and routed IES interfaces due to MPLS packets not contributing to this statistics counter.

Table 53 **Detailed IP Interface Field Descriptions (Continued)**

Label	Description
Rx V4 Discard Pk* Rx V4 Discard Byt*	The total number of IPv4 receive packets or bytes discarded on the interface
Inv Hdr CRC Pkts Inv Hdr CRC Bytes	The number of packets or bytes received on the interface with an invalid IPv4 header CRC value Applies to IPv4 only
Inv Length Pkts Inv Length Bytes	The number of packets or bytes received on the interface with invalid length information in the header. Invalid length information includes an IP header length of less than 20 bytes or greater than the total IP packet length, or an IP packet larger than the Layer 2 frame length.
Inv GRE Protoco* Inv GRE Protocol*	The number of packets or bytes received on the network interface with an unsupported GRE header. The only supported protocol type is MPLS unicast (0x8847). All GRE packets received on an access interface that are meant to be terminated at the node are also discarded for this reason.
Dest Unreach Pk* Dest Unreach Byt*	The number of packets or bytes received on the interface with no route to the destination
Inv Mcast Addr * Inv Mcast Addr B*	The number of packets or bytes discarded on the interface due to unsupported multicast addresses
Directed Bcast * Directed Bcast B*	The number of directed broadcast packets or bytes discarded on the interface when the interface is not enabled for directed broadcast packets Applies to IPv4 only
Src Martian Add* Src Martian Addr*	The number of IPv4 packets or bytes discarded on the interface due to invalid source addresses
Dest Martian Ad* Dest Martian Add*	The number of packets or bytes discarded on the interface due to invalid destination addresses
Black Hole Pkts Black Hole Bytes	The number of packets or bytes discarded on the interface due to blackhole destination addresses
FltrActionDrop P * FltrActionDrop By*	The total number of packets or bytes discarded on the interface by the associated filter. This output field may display N/A for IP/override filter drop statistics that are already collected under a VPLS SAP or spoke SDP.
FltrNHUnreach P* FltrNHUnreach By*	The total number of packets or bytes discarded by policy-based routing when the next hop is unreachable Applies to IPv4 only

Table 53 **Detailed IP Interface Field Descriptions (Continued)**

Label	Description
FltrNHNotDirect* FltrNHNotDirect *	The total number of packets or bytes discarded by policy-based routing when the next hop is not directly connected but a direct hop is configured on the policy-based routing entry Applies to IPv4 only
TTL Expired Pkts TTL Expired Bytes	The total number of packets or bytes discarded on the interface due to TTL expiration
Slowpath Pkts Slowpath Bytes	The number of receive packets and bytes discarded on the interface due to slowpath destination
MTU Exceeded Pk* MTU Exceeded Byt*	The number of receive packets and bytes discarded on the interface due to exceeding the MTU configured on the interface
Queue Pkts Queue Bytes	The number of receive packets and bytes discarded on the interface due to inability to be queued
EncryptionDrop * EncryptionDrop B*	The number of receive packets and bytes discarded on the interface due to an encryption error
Last Tunnel	The name or address of the last tunnel traversed on the received packet
Other Discards * Other Discards B*	The number of receive packets or bytes internally discarded
Rx V6 Pkts Rx V6 Bytes	The number of IPv6 packets or bytes received on the interface. This output field may display N/A for spoke SDP and IES interfaces due to MPLS packets not contributing to this statistics counter.
Rx V6 Discard Pk*	The number of IPv6 receive packets and bytes discarded on the interface See Rx V4 Discard Pk* for field descriptions
Rx V6 Discard Byt*	
Tx Pkts Tx Bytes	The total number of IPv4 and IPv6 packets or bytes sent on the interface. This output field may display N/A for spoke SDP and interfaces due to MPLS packets not contributing to this statistics counter.
Tx V4 Pkts Tx V4 Bytes	The number of IPv4 packets or bytes transmitted on the interface. This output field may display N/A for spoke SDP and IES interfaces due to MPLS packets not contributing to this statistics counter.
Tx V4 Discard Pk* Tx V4 Discard Byt*	The number of IPv4 transmit packets or bytes discarded on the interface.

Table 53 **Detailed IP Interface Field Descriptions (Continued)**

Label	Description
FltrActionDrop * FltrActionDrop B*	The total number of transmit packets or bytes discarded on the interface by the associated filter. This output field may display N/A for IP/override filter drop statistics that are already collected under a VPLS SAP or spoke SDP.
EncryptionDrop * EncryptionDrop B*	The number of transmit packets or bytes discarded by the interface due to an encryption error Applies to IPv4 only
Last Tunnel	The name or address of the last tunnel traversed by the transmitted packet Applies to IPv4 only
Other Discards * Other Discards B*	The number of transmit packets and bytes discarded by the interface due to other reasons
Tx V6 Pkts Tx V6 Bytes	The number of IPv6 packets or bytes transmitted on the interface. This output field may display N/A for spoke SDP and IES interfaces due to MPLS packets not contributing to this statistics counter.
Tx V6 Discard Pk* Tx V6 Discard Byt*	The number of IPv6 transmit packets or bytes discarded on the interface. See Tx V4 Discard Pk* for field descriptions
Security Details	
Admin Zone	Zone ID to which the interface is assigned
Oper Zone	Currently active Zone ID to which the interface is assigned
Bypass	Indicates whether the interface is in security bypass mode
Rx V4 Discard Pk* Rx V4 Discard Byt*	The number of received IPv4 packets or bytes discarded
Unsup Proto Pkts Unsup Proto Bytes	The number of unsupported protocol packets or bytes
Unsup Svc Pkts Unsup Svc Bytes	The number of unsupported service packets or bytes
Unsup ICMP Type* Unsup ICMP Type *	The number of unsupported ICMP packets or bytes
Fragment Pkts Fragment Bytes	The number of dropped packets or bytes due to fragmented packets or bytes

Table 53 **Detailed IP Interface Field Descriptions (Continued)**

Label	Description
No Session Pkts No Session Bytes	The number of dropped packets or bytes dropped due to no session
NAT Rte Loop Pk* NAT Rte Loop Byt*	The number of NAT route loop packets or bytes
Other Discards * Other Discards B*	The number of non-IPv4 packets or bytes discarded
IPV4 GRE Fragmentation and Reassembly Statistics	
Frag Tx Pkts Frag Tx Bytes	The number of fragmented IPv4 GRE-encapsulated packets or bytes transmitted
Frag Rx Pkts Frag Rx Bytes	The number of fragmented IPv4 GRE-encapsulated packets or bytes received
Frag Rx Drp Pkts Frag Rx Drp Bytes	The number of received fragmented IPv4 GRE-encapsulated packets or bytes dropped due to reassembly timeout, reassembly error, or other reasons
ExpiredWait Count	The number of times reassembly timers for the interface have expired
Proxy ARP Details	
Rem Proxy ARP	Indicates whether remote proxy ARP is enabled or disabled
Local Proxy ARP	Indicates whether local proxy ARP is enabled or disabled
Policies	Specifies the policy statements applied to proxy ARP
Proxy Neighbor Discovery Details	
Local Pxy ND	Indicates whether local proxy neighbor discovery (ND) is enabled or disabled
Policies	Specifies the policy statements applied to proxy ND
DHCP Details	
Description	The descriptive text string for the DHCP configuration context
Admin State	Down — the IP interface is administratively disabled
	Up — the IP interface is administratively enabled

Table 53 **Detailed IP Interface Field Descriptions (Continued)**

Label	Description
Action	The relay information policy Keep — the existing information is kept on the packet and the router does not add any additional information
	Replace — on ingress, the existing information-option is replaced with the information-option from the router
Copy to Opt43	Indicates whether vendor-specific information is copied from the DHCP server to the client in Option 43
ICMP Details	
Redirects	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	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	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
IPCP Address Extension Details	
Peer IP Addr	Specifies the remote IP address to be assigned to the far-end via IPCP extensions
Peer Pri DNS Addr	Specifies an IP address for the primary DNS server to be signaled to the far-end via IPCP extensions
Peer Sec DNS Addr	Specifies an IP address for the secondary DNS server to be signaled to the far-end via IPCP extensions. (optional)
DHCP CLIENT Details	
DHCP Client	Indicates whether the interface is enabled as a DHCP client
client-id	The client ID string or n/a if no client identifier has been specified
vendor-id	The vendor class ID value or n/a if no vendor class ID has been specified
Admin Groups	The admin groups associated with this interface

Table 53 **Detailed IP Interface Field Descriptions (Continued)**

Label	Description
Srlg Groups	The SRLG groups associated with this interface
QoS Details	
Egr Queue Pol	The egress queue policy assigned to the interface
Egr Agg RateLimit	The egress aggregate rate limit
Egr Agg Cir	The egress aggregate CIR
Queue Statistics	
Egress Queue	The egress queue for which queue statistics are displayed
In Profile forwarded	The number of packets and octets forwarded by the queue for in-profile and best-effort traffic
In Profile dropped	The number of packets and octets dropped by the queue for in-profile and best-effort traffic
Out Profile forwarded	The number of packets and octets forwarded by the queue for out-of-profile and best-effort traffic
Out Profile dropped	The number of packets and octets dropped by the queue for out-of-profile and best-effort traffic
Group Encryption (MP-BGP) Statistics	
GrpEnc Rx Pkts GrpEnc Rx Bytes	The number of group encryption packets or bytes received
Drp InvSpi Pkts Drp InvSpi Bytes	The number of received group encryption packets or bytes dropped due to an invalid security parameter index (SPI)
Drp Oth Pkts Drp Oth Bytes	The number of received group encryption packets or bytes dropped due to other reasons
GrpEnc Tx Pkts GrpEnc Tx Bytes	The number of group encryption packets or bytes transmitted
Drp pkts Drp bytes	The number of transmitted group encryption packets or bytes dropped

Output Example (statistics)

```
A:7705:Routing-SarA# show router 1 interface  "if_vprn2" statistics
===============================================================================
Interface Statistics
===============================================================================
If Name          : if_vprn2
Admin State      : Up                    Oper (v4/v6)      : Up/Down
Rx Pkts          : 0                     Rx Bytes          : 0
Rx V4 Pkts       : 0                     Rx V4 Bytes       : 0
Rx V4 Discard Pk*: 0                     Rx V4 Discard Byt*: 0
 Inv Hdr CRC Pkts: 0                      Inv Hdr CRC Bytes: 0
 Inv Length Pkts : 0                      Inv Length Bytes : 0
 Inv GRE Protoco*: 0                      Inv GRE Protocol*: 0
 Dest Unreach Pk*: 0                      Dest Unreach Byt*: 0
 Inv Mcast Addr *: 0                      Inv Mcast Addr B*: 0
 Directed Bcast *: 0                      Directed Bcast B*: 0
 Src Martian Add*: 0                      Src Martian Addr*: 0
 Dest Martian Ad*: 0                      Dest Martian Add*: 0
 Black Hole Pkts : 0                      Black Hole Bytes : 0
 FltrActionDrop P*: N/A                   FltrActionDrop By*: N/A
 FltrNHUnreach P*: 0                      FltrNHUnreach By*: 0
 FltrNHNotDirect*: 0                      FltrNHNotDirect *: 0
 TTL Expired Pkts: 0                      TTL Expired Bytes: 0
 Slowpath Pkts   : 0                      Slowpath Bytes   : 0
 MTU Exceeded Pk*: 0                      MTU Exceeded Byt*: 0
 Queue Pkts      : 0                      Queue Bytes      : 0
 EncryptionDrop *: 0                      EncryptionDrop B*: 0
  Last Tunnel    : (Not Specified)
 Other Discards *: 0                      Other Discards B*: 0
Rx V6 Pkts       : 0                     Rx V6 Bytes       : 0
Rx V6 Discard Pk*: 0                     Rx V6 Discard Byt*: 0
 Inv Length Pkts : 0                      Inv Length Bytes : 0
 Dest Unreach Pk*: 0                      Dest Unreach Byt*: 0
 Inv Mcast Addr *: 0                      Inv Mcast Addr B*: 0
 Src Martian Add*: 0                      Src Martian Addr*: 0
 Dest Martian Ad*: 0                      Dest Martian Add*: 0
 Black Hole Pkts : 0                      Black Hole Bytes : 0
 FltrActionDrop P*: N/A                   FltrActionDrop By*: N/A
 TTL Expired Pkts: 0                      TTL Expired Bytes: 0
 Slowpath Pkts   : 0                      Slowpath Bytes   : 0
 MTU Exceeded Pk*: 0                      MTU Exceeded Byt*: 0
 Queue Pkts      : 0                      Queue Bytes      : 0
 EncryptionDrop *: 0                      EncryptionDrop B*: 0
  Last Tunnel    : (Not Specified)
 Other Discards *: 0                      Other Discards B*: 0
Tx Pkts          : 0                     Tx Bytes          : 0
Tx V4 Pkts       : 0                     Tx V4 Bytes       : 0
Tx V4 Discard Pk*: 0                     Tx V4 Discard Byt*: 0
 FltrActionDrop P*: N/A                   FltrActionDrop By*: N/A
 MTU Exceeded Pk*: 0                      MTU Exceeded Byt*: 0
 Queue Pkts      : 0                      Queue Bytes      : 0
 EncryptionDrop *: 0                      EncryptionDrop B*: 0
  Last Tunnel    : (Not Specified)
 Other Discards *: 0                      Other Discards B*: 0
Tx V6 Pkts       : 0                     Tx V6 Bytes       : 0
Tx V6 Discard Pk*: 0                     Tx V6 Discard Byt*: 0
 FltrActionDrop P*: N/A                   FltrActionDrop By*: N/A
 MTU Exceeded Pk*: 0                      MTU Exceeded Byt*: 0
```

```
 Queue Pkts      : 0                    Queue Bytes      : 0
 EncryptionDrop *: 0                    EncryptionDrop B*: 0
  Last Tunnel    : (Not Specified)
 Other Discards *: 0                    Other Discards B*: 0
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:7705:Routing-SarA#
```

Note: The show command syntax for viewing VPRN interface statistics is **show router** *router-instance* **interface** [*ip-address* | *ip-int-name*] **statistics** (for example, **show router 4 interface "vprn_interface" statistics**). The *router-instance* parameter is not required for non-VPRN interfaces.

See Table 53 for field descriptions of the **show router interface statistics** command.

Output Example (security)

```
*A-ALU-1# show router interface ies-201-10.1.0.1 security
===============================================================================
Interface Security
===============================================================================
If Name          : ies-201-10.1.0.1
Admin Zone       : None                 Oper Zone         : None
Bypass           : No
Rx V4 Discard Pk*: 0                    Rx V4 Discard Byt*: 0
 Unsup Proto Pkts: 0                     Unsup Proto Bytes: 0
 Unsup Svc Pkts  : 0                     Unsup Svc Bytes  : 0
 Unsup ICMP Type*: 0                     Unsup ICMP Type *: 0
 Fragment Pkts   : 0                     Fragment Bytes   : 0
 No Session Pkts : 0                     No Session Bytes : 0
 NAT Rte Loop Pk*: 0                     NAT Rte Loop Byt*: 0
 Other Discards *: 0                     Other Discards B*: 0
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A-ALU-1#
```

See Table 53 for field descriptions of the **show router interface security** command.

Output Example (tcp-mss)

```
*A-7705:Duct-C# show router interface Dut-B1_ingress tcp-mss
===============================================================================
TCP MSS Option Adjustment
===============================================================================
If Name          : Dut-B1_ingress
Total (v4/v6)    : 1
  Ok             : 0
  Adjusted       : 1
  Inserted       : 0
  Errors         : 0
Other If MSS Used: 0
  Ingress : 0
  Egress  : 0
```

```
===============================================================================
*A-7705:Duct-C#

*A-7705:Duct-C# show router interface Dut-B1_egress tcp-mss
===============================================================================
TCP MSS Option Adjustment
===============================================================================
If Name          : Dut-B1_egress
Total (v4/v6)    : 0
  Ok           : 0
  Adjusted     : 0
  Inserted     : 0
  Errors       : 0
Other If MSS Used: 1
  Ingress : 1
  Egress  : 0
===============================================================================
*A-7705:Duct-C#
```

Table 54 **IP Interface TCP MSS Adjustment Field Descriptions**

Label	Description
If Name	The name of the interface on which TCP MSS adjustment is configured
Total (v4/v6)	The total number of TCP packets analyzed for TCP MSS adjustment
Ok	The total number of TCP packets whose MSS value was not changed
Adjusted	The total number of TCP packets whose MSS value was adjusted to the MSS value configured on the interface
Inserted	The total number of TCP packets that had the MSS value configured on the interface inserted in the packet header
Errors	The number of packets whose MSS value could not be adjusted or inserted due to an error with the TCP header.
Other If MSS Used Ingress Egress	When both the ingress and egress interfaces have the **tcp-mss** command configured, the interface with the lower of the two configured values is used for comparing against the TCP packet MTU. This statistic indicates the number of packets where the other interface was used for comparing against the TCP packet MTU. The Ingress and Egress fields indicate whether the other interface used was the ingress or egress interface.

neighbor

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

Context show>router

Description This command displays information about the IPv6 neighbor cache.

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

Values 32 characters maximum

ip-address — the address of the IPv6 interface

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

ieee-mac-address — the MAC address

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

summary — displays summary neighbor information

dynamic — displays dynamic IPv6 neighbors

static — displays static IPv6 neighbors

managed — displays managed IPv6 neighbors

Output The following output is an example of IPv6 neighbor information, and Table 55 describes the fields.

Output Example

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

Table 55 **IPv6 Neighbor Field Descriptions**

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

reassembly-profile

Syntax **reassembly-profile** [*profile-id*] [**detail**]

Context show>router

Description This command displays information about all configured reassembly profiles. Executing the command with a *profile-id* will display information only for the specified reassembly profile.

Parameters *profile-id* — reassembly profile ID number

Values 1 to 16

detail — displays detailed profile information

Output The following output is an example of reassembly-profile information, and Table 56 describes the fields.

Output Example

```
*A:7705:Dut-C# show router reassembly-profile
===============================================================================
Reassembly Profiles
===============================================================================
-------------------------------------------------------------------------------
Reassembly Profile (16)
-------------------------------------------------------------------------------
Profile-id       : 16
Description      : (Not Specified)
CBS              : 0 KB
MBS              : 180 KB
Wait (msecs)     : 555
EPD % Threshold  : 50
-------------------------------------------------------------------------------
FC      CBS Override (KB)       MBS Override (KB/B)     Wait Override (msecs)
-------------------------------------------------------------------------------
```

```
No FC Entries Found.
===============================================================================


*A:7705:Dut-C# show router reassembly-profile detail
===============================================================================
Reassembly Profiles
===============================================================================
-------------------------------------------------------------------------------
Reassembly Profile (16)
-------------------------------------------------------------------------------
Profile-id       : 16
Description      : (Not Specified)
CBS              : 0 KB
MBS              : 180 KB
Wait (msecs)     : 555
EPD % Threshold  : 50
-------------------------------------------------------------------------------
FC      CBS Override (KB)       MBS Override (KB/B)     Wait Override (msecs)
-------------------------------------------------------------------------------
No FC Entries Found.
-------------------------------------------------------------------------------
Interface Associations
-------------------------------------------------------------------------------
Interface      : ip-10.12.1.2
IP Addr.         : 10.12.1.2/30           Port Id          : 1/1/2
Interface      : ip-10.12.1.6
IP Addr.         : 10.12.1.6/30           Port Id          : 1/1/2
-------------------------------------------------------------------------------
===============================================================================
*A:7705:Dut-C#
```

Table 56 **Reassembly Profile Field Descriptions**

Label	Description
Profile-id	The reassembly profile ID number
Description	The configured reassembly profile description
CBS	The configured CBS value for the reassembly profile
MBS	The configured MBS value for the reassembly profile
Wait (msecs)	The configured wait time for the reassembly profile
EPD % Threshold	The configured EPD threshold for the reassembly profile
FC	The forwarding classes configured under the reassembly profile
CBS Override (KB)	The configured CBS override value for the forwarding class
MBS Override (KB/B)	The configured MBS override value for the forwarding class
Wait Override (msecs)	The configured wait time override for the forwarding class

Table 56 **Reassembly Profile Field Descriptions (Continued)**

Label	Description
Interface Associations	
Interface	The associated interface name
IP Addr.	The IP address of the associated interface
Port Id	The port used by the associated interface

route-next-hop-policy

Syntax **route-next-hop-policy template**

Context show>router

Description This command displays information about the route next-hop policy template.

Output The following output is an example of route next-hop policy template information, and Table 57 describes the fields.

Output Example

```
*A:ALU# show router route-next-hop-policy template
===============================================================================
Route next-hop templates
===============================================================================
Template                          Description
-------------------------------------------------------------------------------
"route-policy-1"                  "template for route policy 1"
-------------------------------------------------------------------------------
Templates : 1
===============================================================================
*A:ALU-A#

*A:ALU# show router route-next-hop-policy template “route-policy-1”
        template "route-policy-1"
            description "template for route policy 1"
            nh-type tunnel
            protection-type link
            srlg-enable
            include-group "group1"
            exclude-group "group2"
        exit
```

Table 57 **Route-next-hop-policy Template Field Descriptions**

Label	Description
Template	The name of the route next-hop policy template
Description	The template description
Templates	The number of configured templates

route-table

Syntax **route-table** [*family*] [*ip-prefix*[*/prefix-length*] [**longer** | **exact** | **protocol** *protocol-name*] [**all**]] [**next-hop-type** *type*] [**alternative**]
route-table [*family*] **summary**
route-table [*family*] [*ip-prefix*[*/prefix-length*]] [**longer** | **exact** | **protocol** *protocol-name*] extensive [**all**]

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.

The following adapter cards and platforms support the full IPv6 subnet range for IPv6 static routes:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card, version 2 and version 3
- 2-port 10GigE (Ethernet) Adapter card (on the v-port)
- 10-port 1GigE/1-port 10GigE X-Adapter card
- 7705 SAR-X

For these cards and platforms, the supported route range for statically provisioned or dynamically learned routes is from /1 to /128.

For all other cards, modules, and ports (including the v-port on the 2-port 10GigE (Ethernet) module), the supported range for statically provisioned or dynamically learned routes is from /1 to /64 or is /128 (indicating a host route).

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

Values **ipv4** — displays the routes that have the IPv4 family enabled, excluding IP-VPN routes

ipv6 — displays the routes that are IPv6-capable, including IPv6 static routes

mcast-ipv4 — displays the routes that are IPv4 multicast-capable

mcast-ipv6 — displays the routes that are IPv6 multicast-capable

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

Values	*ipv4-prefix*	a.b.c.d (host bits must be 0)
	ipv4-prefix-length	0 to 32
Values	*ipv6-prefix*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	ipv6-prefix-length	{0 to 128} | {0 to 64 | 128}

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

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

protocol-name — displays routes learned from the specified protocol

Values bgp, bgp-vpn, isis, local, nat, ospf, rip, static, aggregate, vpn-leak, managed

all — displays all routes, including inactive routes

type — displays tunneled next-hop information

alternative — displays LFA and backup route details

extensive — displays next-hop FIB information for the route table

summary — displays route table summary information

Output The following outputs are examples of routing table information:

- standard and extensive route table information (Output Example, Table 58)
- LFA and backup route table information (Output Example, Table 59)

Output Example

```
*A:ALU# show router route-table
===============================================================================
Route Table (Router: Base)
===============================================================================
Dest Prefix[Flags]                              Type    Proto    Age         Pref
       Next Hop[Interface Name]                                       Metric
-------------------------------------------------------------------------------
10.0.0.0/0                                    Remote  Static    00h00m03s  5
       upLink                                                     1
10.1.1.1/32                                   Local   Local    35d08h00m   0
       system                                                     0
-------------------------------------------------------------------------------
No. of Routes: 1
Flags: n = Number of times nexthop is repeated
       Backup = BGP backup route
       LFA = Loop-Free Alternate nexthop
       S = Sticky ECMP requested
```

```
===============================================================================
*A:Sar18 Dut-B>show>router#

*A:ALU-A# show router route-table protocol ospf
===============================================================================
Route Table  (Router: Base)
===============================================================================
Dest Prefix[Flags]                            Type    Proto    Age        Pref
       Next Hop[Interface Name]                                      Metric
-------------------------------------------------------------------------------
10.10.0.1/32                                   Remote  OSPF    65844        10
       10.10.13.1                                                       0
-------------------------------------------------------------------------------
Flags: n = Number of times nexthop is repeated
       Backup = BGP backup route
       LFA = Loop-Free Alternate nexthop
       S = Sticky ECMP requested
===============================================================================
*A:Sar18 Dut-B>show>router#

*A:ALU-A# show router route-table protocol nat
===============================================================================
Route Table  (Router: Base)
===============================================================================
Dest Prefix[Flags]                          Type    Proto   Age        Pref
       Next Hop[Interface Name]                                Metric
-------------------------------------------------------------------------------
200.1.1.5/32                                Remote  NAT     00h00m20s  0
       100.1.1.10                                               0
200.1.1.6/31                                Remote  NAT     00h00m20s  0
       100.1.1.11                                               0
200.1.1.8/29                                Remote  NAT     00h00m20s  0
       100.1.1.13                                               0
200.1.1.16/28                               Remote  NAT     00h00m20s  0
       100.1.1.21                                               0
200.1.1.32/29                               Remote  NAT     00h00m20s  0
       100.1.1.37                                               0
200.1.1.40/30                               Remote  NAT     00h00m20s  0
       100.1.1.45                                               0
200.1.1.44/31                               Remote  NAT     00h00m20s  0
       100.1.1.49                                               0
-------------------------------------------------------------------------------
No. of Routes: 7
Flags: n = Number of times nexthop is repeated
       B = BGP backup route available
       L = LFA nexthop available
===============================================================================
*A:SarA Dut-B>show>router#

*A:7705:Dut-C# show router 1 route-table  extensive
===============================================================================
Route Table (Service: 1)
===============================================================================
Dest Prefix             : 10.1.13.0/24
  Protocol              : BGP_VPN
  Age                   : 00h01m05s
  Preference            : 170
  Indirect Next-Hop     : 10.20.1.1
```

```
    Label               : 131070
    QoS                 : Priority=n/c, FC=n/c
    Source-Class        : 0
    Dest-Class          : 0
    ECMP-Weight         : N/A
    Resolving Next-Hop  : 10.20.1.1 (RSVP tunnel:1)
      Metric            : 1000
      ECMP-Weight       : N/A
-------------------------------------------------------------------------------
Dest Prefix             : 10.1.14.0/24
  Protocol              : BGP_VPN
  Age                   : 00h00m58s
  Preference            : 170
  Indirect Next-Hop     : 10.20.1.2
    Label               : 131070
    QoS                 : Priority=n/c, FC=n/c
    Source-Class        : 0
    Dest-Class          : 0
    ECMP-Weight         : N/A
    Resolving Next-Hop  : 10.20.1.2 (RSVP tunnel:2)
      Metric            : 1000
      ECMP-Weight       : N/A
-------------------------------------------------------------------------------
Dest Prefix             : 10.1.15.0/24
  Protocol              : LOCAL
  Age                   : 00h11m02s
  Preference            : 0
  Next-Hop              : N/A
    Interface           : ies-1-10.1.15.3
    QoS                 : Priority=n/c, FC=n/c
    Source-Class        : 0
    Dest-Class          : 0
    Metric              : 0
    ECMP-Weight         : N/A
-------------------------------------------------------------------------------
<snip>
*A:7705:Dut-C#
```

Table 58 **Standard and Extensive Route Table Field Descriptions**

Label	Description
Dest Prefix	The route destination address and mask
[Flags]	n — Number of times **nexthop** is repeated Backup — BGP backup route LFA — Loop-free alternate next hop S — Sticky ECMP requested
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
Protocol	The protocol through which the route was learned

Table 58 **Standard and Extensive Route Table Field Descriptions**

Label	Description
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
Interface	The interface name of the next hop
QoS	The FC and priority associated with the next hop
Source-Class	The source class value, 0 to 255
Dest-Class	The destination class value, 0 to 255
ECMP-Weight	The fractional share of bandwidth for the next hop, either N/A or 1 to 32
No. of Destinations	The total number of next-hop destinations

Output Example

```
*A:ALU# show router route-table alternative
===============================================================================
Route Table (Router: Base)
===============================================================================
Dest Prefix[Flags]                              Type    Proto    Age          Pref
       Next Hop[Interface Name]                                    Metric
       Alt-NextHop                                                 Alt-
                                                                   Metric
-------------------------------------------------------------------------------
10.10.1.0/24                                    Local   Local    00h07m52s   0
       ip-10.10.1.1                                                 0
10.10.2.0/24                                    Local   Local    00h07m48s   0
       ip-10.10.2.1                                                 0
10.10.4.0/24                                    Remote  ISIS     00h07m38s   15
       10.10.1.2                                                    20
10.10.5.0/24                                    Remote  ISIS     00h07m38s   15
       10.10.2.3                                                    20
10.10.9.0/24                                    Remote  ISIS     00h07m28s   15
       10.10.1.2                                                    30
       10.20.1.5 (LFA) (tunneled:RSVP:3)                            50
10.10.10.0/24                                   Remote  ISIS     00h04m40s   15
       10.20.1.5 (tunneled:RSVP:3)                                  30
10.20.1.1/32                                    Local   Local    00h07m55s   0
       system                                                       0
10.20.1.2/32                                    Remote  ISIS     00h07m47s   15
       10.10.1.2                                                    10
10.20.1.3/32                                    Remote  ISIS     00h07m38s   15
       10.10.2.3                                                    10
10.20.1.4/32                                    Remote  ISIS     00h07m38s   15
       10.10.1.2                                                    20
```

```
       10.20.1.5 (LFA) (tunneled:RSVP:3)                                40
10.20.1.5/32                                    Remote  ISIS     00h04m40s   15
       10.20.1.5 (tunneled:RSVP:3)                                      20
10.20.1.6/32                                    Remote  ISIS     00h07m28s   15
       10.10.1.2                                                        30
       10.10.2.3 (LFA)                                                  30
-------------------------------------------------------------------------------
No. of Routes: 12
Flags: n = Number of times nexthop is repeated
       Backup = BGP backup route
       LFA = Loop-Free Alternate nexthop
       S = Sticky ECMP requested
===============================================================================
*A:ALU-A#
```

Table 59 **LFA and Backup Route Table Field Descriptions**

Label	Description
Dest Prefix[Flags]	The route destination address and mask, and flags (if applicable)
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
Alt-NextHop	The backup next hop
Alt-Metric	The metric of the backup route

rtr-advertisement

Syntax **rtr-advertisement** [**interface** *interface-name*] [**prefix** *ipv6-prefix/prefix-length*] [**conflicts**]

Context show>router

Description This command displays router advertisement information. If no parameters are specified, all routes are displayed, sorted by prefix.

Parameters *interface-name* — the interface name

Values 32 characters maximum

ipv6-prefix/prefix-length — displays only those routes matching the specified IP prefix and prefix length

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

conflicts — displays router advertisement conflicts

Output The following output is an example of router advertisement information, and Table 60 describes the fields.

Output Example

```
*A:ALU-A# show router rtr-advertisement
===============================================================================
Router Advertisement
-------------------------------------------------------------------------------
Interface: interfaceNetworkNonDefault
-------------------------------------------------------------------------------
Rtr Advertisement Tx : 8                Last Sent            : 00h01m28s
Nbr Solicitation Tx  : 83               Last Sent            : 00h00m17s
Nbr Advertisement Tx : 74               Last Sent            : 00h00m25s
Rtr Advertisement Rx : 8                Rtr Solicitation Rx  : 0
Nbr Advertisement Rx : 83               Nbr Solicitation Rx  : 74
-------------------------------------------------------------------------------
Max Advert Interval  : 601              Min Advert Interval  : 201
Managed Config       : TRUE             Other Config         : TRUE
Reachable Time       : 00h00m00s400ms   Router Lifetime      : 00h30m01s
Retransmit Time      : 00h00m00s400ms   Hop Limit            : 63
Link MTU             : 1500
MAC Addr To Use      : Interface

Prefix: 3::/64
Autonomous Flag      : FALSE            On-link flag         : FALSE
Preferred Lifetime   : 07d00h00m        Valid Lifetime       : 30d00h00m

Prefix: 16::/64
Autonomous Flag      : FALSE            On-link flag         : FALSE
Preferred Lifetime   : 49710d06h        Valid Lifetime       : 49710d06h
-------------------------------------------------------------------------------
Advertisement from: FE80::200:FF:FE00:2
Managed Config       : FALSE            Other Config         : FALSE
Reachable Time       : 00h00m00s0ms     Router Lifetime      : 00h30m00s
Retransmit Time      : 00h00m00s0ms     Hop Limit            : 64
Link MTU             : 0
-------------------------------------------------------------------------------
*A:ALU-A#
```

Table 60 **Router Advertisement Field Descriptions**

Label	Description
Rtr Advertisement Tx/Last Sent	The number of router advertisements sent and the time they were sent
Nbr Solicitation Tx/Last Sent	The number of neighbor solicitation messages sent and the time they were sent
Nbr Advertisement Tx/Last Sent	The number of neighbor advertisements sent and the time they were sent
Rtr Advertisement Rx	The number of router advertisements received
Rtr Solicitation Rx	The number of router solicitation messages received
Nbr Advertisement Rx	The number of neighbor advertisements received
Nbr Solicitation Rx	The number of neighbor solicitation messages received
Max Advert Interval	The maximum interval between sending router advertisement messages
Min Advert Interval	The minimum interval between sending router advertisement messages
Managed Config	True — DHCPv6 has been configured
	False — DHCPv6 is not available for address configuration
Other Config	True — there are other stateful configurations
	False — there are no other stateful configurations
Reachable Time	The time, in milliseconds, that a node assumes a neighbor is reachable after receiving a reachability confirmation
Router Lifetime	The router lifetime, in seconds
Retransmit Time	The time, in milliseconds, between retransmitted neighbor solicitation messages
Hop Limit	The current hop limit
Link MTU	The MTU number that the nodes use for sending packets on the link
Autonomous Flag	True — the prefix can be used for stateless address autoconfiguration
	False — the prefix cannot be used for stateless address autoconfiguration

Table 60 **Router Advertisement Field Descriptions (Continued)**

Label	Description
On-link flag	True — the prefix can be used for onlink determination
	False — the prefix cannot be used for onlink determination
Preferred Lifetime	The remaining time, in seconds, that this prefix will continue to be preferred
Valid Lifetime	The length of time, in seconds, that the prefix is valid for the purpose of onlink determination

static-arp

Syntax **static-arp** [*ip-address* | *ip-int-name* | **mac** *ieee-mac-addr*]

Context show>router

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

If no options are present, all ARP entries are displayed.

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

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

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

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

Output The following output is an example of the static ARP table, and Table 61 describes the fields.

Output Example

```
*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
10.200.1.1      00:00:5a:01:00:33 00:00:00    Inv  to-ser1a
-------------------------------------------------------------------------------
No. of ARP Entries: 1
===============================================================================
```

```
*A:ALU-A# show router static-arp 10.200.1.1
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Expiry      Type Interface
-------------------------------------------------------------------------------
10.200.1.1      00:00:5a:01:00:33 00:00:00    Inv  to-ser1a

===============================================================================
*A:ALU-A#
```

Table 61 **Static ARP Table Field Descriptions**

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

static-route

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

Context show>router

Description This command displays the static entries in the routing table.

If no options are present, all static routes are displayed sorted by prefix.

The following adapter cards and platforms support the full IPv6 subnet range for IPv6 static routes:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card, version 2 and version 3
- 2-port 10GigE (Ethernet) Adapter card (on the v-port)
- 10-port 1GigE/1-port 10GigE X-Adapter card
- 7705 SAR-X

For these cards and platforms, the supported route range for statically provisioned or dynamically learned routes is from /1 to /128.

For all other cards, modules, and ports (including the v-port on the 2-port 10GigE (Ethernet) module), the supported range for statically provisioned or dynamically learned routes is from /1 to /64 or is /128 (indicating a host route).

Parameters *family* — displays the specified router IP interface family

Values ipv4, ipv6, mcast-ipv4, or mcast-ipv6

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

Values	*ipv4-prefix*	a.b.c.d (host bits must be 0)
	ipv4-prefix-length	0 to 32
Values	*ipv6-prefix*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D
	ipv6-prefix-length	{0 to 128} | {0 to 64 | 128}

preference — only displays static routes with the specified route preference

Values 0 to 65535

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

Values	*ipv4-address*	a.b.c.d (host bits must be 0)
Values	*ipv6-address*	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

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

Values 1 to 4294967295

detail — displays detailed static route information

Output The following output is an example of static route information, and Table 62 describes the fields.

Output Example

```
*A:ALU-1# show router static-route
===============================================================================
Static Route Table (Router: Base)  Family: IPv4
===============================================================================
Prefix                                    Tag         Met    Pref Type Act
   Next Hop                                Interface
-------------------------------------------------------------------------------
```

```
192.168.250.0/24                                        1      5     NH   Y
   10.200.10.1                                  to-ser1
192.168.252.0/24                                        1      5     NH   N
   10.10.0.254                                  n/a
192.168.253.0/24                                        1      5     NH   N
    to-ser1                                     n/a
===============================================================================
*A:ALU-A#
```

Table 62 **Static Route Table Field Descriptions**

Label	Description
Prefix	The static route destination address
Tag	The 32-bit integer tag added to the static route
Met	The route metric value for the static route
Pref	The route preference value for the static route
Type	NH — The route is a static route with a directly connected next hop. The next hop for this type of route is either the next-hop IP address or an egress IP interface name.
Act	N — the static route is inactive; for example, the static route is disabled or the next-hop IP interface is down
	Y — the static route is active
Next Hop	The next hop for the static route destination
No. of Routes	The number of routes displayed in the list

status

Syntax **status**

Context show>router

Description This command displays the router status.

Output The following output is an example of router status information, and Table 63 describes the fields.

Output Example

```
*A:ALU-1# show router status
===============================================================
Router Status (Router: Base)
===============================================================
                         Admin State         Oper State
```

```
---------------------------------------------------------------
Router                    Up                  Up
OSPFv2-0                  Up                  Up
RIP                       Up                  Up
ISIS                      Up                  Up
MPLS                      Up                  Up
RSVP                      Up                  Down
LDP                       Up                  Down
BGP                       Up                  Up

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

Table 63 **Router Status Field Descriptions**

Label	Description
Router	The administrative and operational states for the router
OSPFv2-0	The administrative and operational states for the OSPF protocol
RIP	The administrative and operational states for the RIP protocol
ISIS	The administrative and operational states for the IS-IS protocol
MPLS	The administrative and operational states for the MPLS protocol
RSVP	The administrative and operational states for the RSVP protocol
LDP	The administrative and operational states for the LDP protocol
BGP	The administrative and operational states for the BGP protocol
Max IPv4 Routes	The maximum number of IPv4 routes configured for the system; local, host, static, and aggregate routes are not counted
Max IPv6 Routes	The maximum number of IPv6 routes configured for the system; local, host, static, and aggregate routes are not counted
Total IPv4 Routes	The number of IPv4 dynamically learned routes in the route table; local, host, static, and aggregate routes are not counted
Total IPv6 Routes	The number of IPv6 dynamically learned routes in the route table; local, host, static, and aggregate routes are not counted

Table 63 **Router Status Field Descriptions (Continued)**

Label	Description (Continued)
ECMP Max Routes	The number of ECMP routes configured for path sharing
Triggered Policies	No — triggered route policy re-evaluation is disabled
	Yes — triggered route policy re-evaluation is enabled

tunnel-table

Syntax **tunnel-table summary** [**ipv4** | **ipv6**]
tunnel-table [**protocol** *protocol*] {**ipv4** | **ipv6**}
tunnel-table [*ip-prefix*[*/mask*]] [**alternative**] [**ipv4** | **ipv6**] **detail**
tunnel-table [*ip-prefix*[*/mask*]] [**alternative**]
tunnel-table [*ip-prefix*[*/mask*]] **protocol** *protocol* [**detail**]
tunnel-table [*ip-prefix*[*/mask*]] **sdp** *sdp-id*

Context show>router

Description This command displays tunnel table information.

When the **auto-bind-tunnel** command is used when configuring a VPRN service, it means the MP-BGP NH resolution is referring to the core routing instance for IP reachability. For a VPRN service, the next hop specifies the lookup to be used by the routing instance if no SDP to the destination exists.

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

Values

ipv4-prefix:	a.b.c.d
ipv4-prefix-length:	[0 to 30]
ipv6-prefix:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D
ipv6-prefix-length:	[0 to 126]

protocol — displays protocol information

Values bgp, ldp, rsvp, sdp, ospf, isis, sr-te, fpe

sdp-id — displays information pertaining to the specified SDP

Values 1 to 17407

summary — displays summary tunnel table information

detail — displays detailed tunnel table information

alternative — displays backup route details

ipv4 — displays information for IPv4 entries only

ipv6 — displays information for IPv6 entries only

Output The following output is an example of tunnel table information, and Table 64 describes the fields.

Output Example

```
*A:Sar18 Dut-B>show>router# tunnel-table summary
===============================================================================
Tunnel Table Summary (Router: Base)
===============================================================================
                              Active                  Available
-------------------------------------------------------------------------------
LDP                           1                       1
SDP                           1                       1
RSVP                          0                       0
BGP                           0                       0
MPLS-TP                       0                       0
ISIS                          0                       0
OSPF                          0                       0
SR-TE                         0                       0
FPE                           0                       0
-------------------------------------------------------------------------------
Total                         2                       2
===============================================================================
*A:Sar18 Dut-B>show>router#

A:Sar18 Dut-B>show>router# tunnel-table
===============================================================================
IPv4 Tunnel Table (Router: Base)
===============================================================================
Destination       Owner     Encap TunnelId  Pref     Nexthop        Metric
-------------------------------------------------------------------------------
1.1.1.1/32       sdp       MPLS  1000      5        1.1.1.1       0
1.1.1.1/32       ldp       MPLS  65537     9        10.1.1.1      1
-------------------------------------------------------------------------------
Flags: B = BGP backup route available
       E = inactive best-external BGP route
===============================================================================
*A:Sar18 Dut-B>show>router#

*A:Sar18 Dut-B>show>router# tunnel-table detail
===============================================================================
Tunnel Table (Router: Base)
===============================================================================
Destination      : 1.1.1.1/32
NextHop          : 10.1.1.1
Tunnel Flags     : (Not Specified)
Age              : 26d21h16m
CBF Classes      : (Not Specified)
Owner            : sdp                 Encap            : MPLS
Tunnel ID        : 1000                Preference       : 5
Tunnel Label     :  -                  Tunnel Metric    : 0
Tunnel MTU       : 1546                Max Label Stack  : 1
-------------------------------------------------------------------------------
```

```
Destination      : 1.1.1.1/32
NextHop          : 10.1.1.1
Tunnel Flags     : (Not Specified)
Age              : 26d21h16m
CBF Classes      : (Not Specified)
Owner            : ldp                  Encap            : MPLS
Tunnel ID        : 65537                Preference       : 9
Tunnel Label     : 131071               Tunnel Metric    : 1
Tunnel MTU       : 1550                 Max Label Stack  : 1
-------------------------------------------------------------------------------
Number of tunnel-table entries          : 2
Number of tunnel-table entries with LFA : 0
===============================================================================
*A:Sar18 Dut-B>show>router#

*A:Sar18 Dut-B>show>router# tunnel-table ipv6 protocol isis
===============================================================================
IPv6 Tunnel Table (Router: Base)
===============================================================================
Destination                                Owner     Encap TunnelId   Pref
Nexthop                                                    Metric
-------------------------------------------------------------------------------
No Matching Entries.
-------------------------------------------------------------------------------
Flags: B = BGP backup route available
       E = inactive best-external BGP route
===============================================================================
*A:Sar18 Dut-B>show>router#
```

Table 64 Tunnel Table Field Descriptions

Label	Description
Destination	The route’s destination address and mask
Owner	Specifies the tunnel owner (protocol)
Encap	Specifies the tunnel’s encapsulation type
Tunnel ID	Specifies the tunnel (SDP) identifier
Pref Preference	Specifies the route preference for routes learned from the configured peers
Nexthop	The next hop for the route’s destination
Metric	The route metric value for the route
CBF Classes	Not applicable
Tunnel Flags	Indicates the tunnel flags
Tunnel Label	Specifies the tunnel label
Tunnel Metric	Specifies the tunnel metric

Table 64 **Tunnel Table Field Descriptions (Continued)**

Label	Description
Tunnel MTU	Specifies the tunnel MTU
Max Label Stack	Indicates the maximum label stack depth
Age	Specifies the tunnel age (that is, how long the tunnel has been operational)

twamp-light

Syntax **twamp-light**

Context show>router

Description This command displays OAM TWAMP Light status information.

Output The following output is an example of TWAMP Light information, and Table 65 describes the fields.

Output Example

```
*A:ALU-3# show router twamp-light
===============================================================================
TWAMP Light Reflector
===============================================================================
Admin State          : Up
Up Time              : 0d 00:12:01
Configured UDP Port  : 65535
Test Packets Rx      : 0                  Test Packets Tx     : 0

TWAMP Light Controller Prefix List
 192.168.1.1/32
    10.1.1.2/32
 172.16.254.9/3
    10.1.1.0/24
===============================================================================
*A:ALU-3#
```

Table 65 **TWAMP Light Field Descriptions**

Label	Description
TWAMP Light Reflector	
Admin State	Displays one of the following: Up—the server or prefix is administratively enabled (no shutdown) in configuration Down—the server or prefix is administratively disabled (shutdown) in configuration
Up Time	The time since the server process was started, measured in days (d), hours, minutes, and seconds
Configured UDP Port	The UDP port number used
Test Packets Rx	The total number of test packets received from session senders
Test Packets Tx	The total number of test packets sent to session senders
TWAMP Light Controller Prefix List	The IP address prefixes of TWAMP Light clients

3.11.2.3 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 options specified.

Parameters **all** — clears all ARP cache entries

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

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 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

dhcp

Syntax **dhcp**

Context clear>router

Description This command enables the context to clear and reset DHCP entities.

dhcp6

Syntax **dhcp6**

Context clear>router

Description This command enables the context to clear and reset DHCPv6 entities.

local-dhcp-server

Syntax **local-dhcp-server** *server-name*

Context clear>router>dhcp
clear>router>dhcp6

Description This command clears DHCP or DHCPv6 server data.

Parameters *server-name* — the name of a local DHCP or DHCPv6 server

declined-addresses

Syntax **declined-addresses** *ip-address*[**/***mask*]
declined-addresses pool *pool-name*

Context clear>router>dhcp>local-dhcp-server

Description This command clears declined DHCP addresses or pools.

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

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

mask — the subnet mask in Classless Inter-Domain Routing (CIDR) notation, expressed as a decimal integer

Values 0 to 32

pool-name — the name of the IP address pool

Values up to 32 alphanumeric characters

leases

Syntax **leases** *ip-address*[**/***mask*] [*state*]
leases [*ipv6-address***/***prefix-length*] [*type*] [*state*]
leases all [*type*] [*state*]

Context clear>router>dhcp>local-dhcp-server
clear>router>dhcp6>local-dhcp-server

Description This command clears the specified DHCP or DHCPv6 leases.

Parameters *ip-address* — the IPv4 address of the leases to clear

mask — the subnet mask, expressed as a decimal integer

Values 0 to 32

ipv6-address/prefix-length — the IPv6 address of the leases to clear

type — the type of the lease to remove (DHCPv6 only)

Values pd | slaac | wan

state — the state of the lease to remove

Values DHCP: offered | remove-pending | internal | internal-orphan
DHCPv6: advertised | remove-pending | held | internal | internal-orphan | internal-offered

all — keyword to remove all leases of the specified type and state

pool-ext-stats

Syntax **pool-ext-stats** [*pool-name*]

Context clear>router>dhcp>local-dhcp-server
clear>router>dhcp6>local-dhcp-server

Description This command resets the collection interval for peak value statistics displayed by the **show router dhcp local-dhcp-server pool-ext-stats** or the **show router dhcp6 local-dhcp-server pool-ext-stats** commands.

Parameters *pool-name* — the name of the local DHCPv6 server pool

prefix-ext-stats

Syntax **prefix-ext-stats** *ipv6-address*/*prefix-length*
prefix-ext-stats pool *pool-name*

Context clear>router>dhcp6>local-dhcp-server

Description This command resets the collection interval for peak value statistics displayed by the **show router dhcp6 local-dhcp-server prefix-ext-stats** command.

Parameters *ipv6-address/prefix-length* — the IPv6 address

pool-name — the name of the local DHCPv6 server pool

server-stats

Syntax **server-stats**

Context clear>router>dhcp>local-dhcp-server
clear>router>dhcp6>local-dhcp-server

Description This command clears all DHCP or DHCPv6 server statistics.

subnet-ext-stats

Syntax **subnet-ext-stats** *ip-address*[/*mask*]
subnet-ext-stats pool *pool-name*

Context clear>router>dhcp>local-dhcp-server

Description This command clears extended subnet statistics.

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

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

mask — the subnet mask in Classless Inter-Domain Routing (CIDR) notation, expressed as a decimal integer

Values 0 to 32

pool-name — the name of the local DHCP server pool

statistics

Syntax **statistics** [*ip-int-name* | *ip-address*]
statistics

Context clear>router>dhcp
clear>router>dhcp6

Description This command clears statistics for DHCP and DHCPv6 Relay.

If no interface name or IP address is specified, statistics are cleared for all configured interfaces.

Parameters *ip-int-name* — 32 characters maximum

ip-address — IPv4 or IPv6 address

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

icmp6

Syntax **icmp6 all**
icmp6 global
icmp6 interface *interface-name*

Context clear>router

Description This command clears ICMPv6 statistics.

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

Parameters **all** — all statistics

global — global statistics

interface-name — 32 characters maximum

interface

Syntax **interface** [*ip-int-name* | *ip-addr*] [**icmp**]
interface *spoke-name* **statistics**

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 interfaces used for ICMP rate limiting

spoke-name — the spoke SDP interface name

neighbor

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

Context clear>router

Description This command clears IPv6 neighbor information.

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

Parameters **all** — all IPv6 neighbors

ip-address — an IPv6 neighbor address

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

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

router-advertisement

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

Context clear>router

Description This command clears router advertisement counters.

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

Parameters **all** — all interfaces

interface-name — 32 characters maximum

3.11.2.4 Debug Commands

destination

Syntax **destination** *trace-destination*

Context debug>trace

Description This command specifies the destination of trace messages.

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

Values stdout, console, logger, memory

enable

Syntax [**no**] **enable**

Context debug>trace

Description This command enables the trace.

The **no** form of the command disables the trace.

trace-point

Syntax [**no**] **trace-point** [**module** *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*
router service-name *service-name*

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	

service-name — specifies the service name, 64 characters maximum

ip

Syntax [**no**] **ip**

Context debug>router

Description This command configures debugging for IP.

arp

Syntax [**no**] **arp**

Context debug>router>ip

Description This command enables or disables ARP debugging.

dhcp

Syntax [**no**] **dhcp** [**interface** *ip-int-name*]
[**no**] **dhcp mac** *ieee-address*
[**no**] **dhcp sap** *sap-id*

Context debug>router>ip

Description This command enables the context for DHCP debugging.

Parameters *ip-int-name* — specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within the double quotes.

ieee-address — specifies a MAC address

sap-id — specifies a SAP identifier

dhcp6

Syntax **dhcp6** [*ip-int-name*]
no dhcp6

Context debug>router>ip

Description This command enables DHCPv6 debugging.

The **no** form of the command disables DHCPv6 debugging.

Parameters *ip-int-name* — specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the strong contains special characters (#, $, spaces, etc.), the entire string must be enclosed within the double quotes.

detail-level

Syntax **detail-level** {**low** | **medium** | **high**}
no detail-level

Context debug>router>ip>dhcp
debug>router>ip>dhcp6
debug>router>local-dhcp-server

Description This command enables debugging for the DHCP or DHCPv6 tracing detail level.

The **no** form of the command disables debugging.

mode

Syntax **mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}
no mode

Context debug>router>ip>dhcp
debug>router>ip>dhcp6
debug>router>local-dhcp-server

Description This command enables debugging for the DHCP or DHCPv6 tracing mode.

The **no** form of the command disables debugging.

icmp

Syntax [**no**] **icmp**

Context debug>router>ip

Description This command enables or disables ICMP debugging.

icmp6

Syntax **icmp6** [*ip-int-name*]
no icmp6

Context debug>router>ip

Description This command enables or disables ICMPv6 debugging. If an interface is specified, debugging only occurs on that interface.

Parameters *ip-int-name* — only debugs the specified IP interface

Values 32 characters maximum

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 debugs the specified IP interface

Values 32 characters maximum

ip-address — only debugs the specified IPv4 or IPv6 address

Values		
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x: [0 to FFFF]H
		d: [0 to 255]D

neighbor

Syntax [**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 debugs the specified IP interface

Values 32 characters maximum

ip-address — only debugs the specified IPv4 or IPv6 address

Values *ipv4-address* a.b.c.d
ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D

headers — only debugs the packet header

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

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

route-table

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

Context debug>router>ip

Description This command configures route table debugging.

The following adapter cards and platforms support the full IPv6 subnet range for IPv6 static routes:

- 6-port Ethernet 10Gbps Adapter card
- 8-port Gigabit Ethernet Adapter card, version 2 and version 3
- 2-port 10GigE (Ethernet) Adapter card (on the v-port)

- 10-port 1GigE/1-port 10GigE X-Adapter card
- 7705 SAR-X

For these cards and platforms, the supported route range for statically provisioned or dynamically learned routes is from /1 to /128.

For all other cards, modules, and ports (including the v-port on the 2-port 10GigE (Ethernet) module), the supported range for statically provisioned or dynamically learned routes is from /1 to /64 or is /128 (indicating a host route).

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

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

Values *ipv6-prefix* x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D
ipv6-prefix-length {0 to 128} | {0 to 64 | 128}

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

local-dhcp-server

Syntax [**no**] **local-dhcp-server** *server-name* [**lease-address** *ip-prefix*[*Iprefix-length*]]
[**no**] **local-dhcp-server** *server-name* [**mac** *ieee-address*]
[**no**] **local-dhcp-server** *server-name* **link-local-address** *ipv6z-address*

Context debug>router

Description This command enables, disables, and configures debugging for a local DHCP server.

Parameters *server-name* — specifies a local DHCP server name

Values 32 characters maximum

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

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

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

ieee-address — specifies a leased MAC address

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx (cannot be all zeros)

ipv6z-address — specifies a leased IPv6 address and an interface name

Values *ipv6z-address* x:x:x:x:x:x:x:x-*interface*
x:x:x:x:x:x:d.d.d.d-*interface*
x: [0 to FFFF]H
d: [0 to 255]D
interface: 32 characters max

custom-format

Syntax **custom-format**

Context debug>security>capture

Description This command enables access to the context to configure custom formatting parameters. Users can input packets into Wireshark in order to provide further debug capabilities.

Packets in various formats, such as PCAP and K12, can be input into Wireshark.

The following is an example of how packets are input into Wireshark in K12 text format. Only the IP header is displayed; the Layer 2 header is not shown in the output for any format command mode (**custom** | **decode** | **raw**).

Note:

- The Layer 2 header is not output by the Firewall; however, since Wireshark K12 expects this field, the header field is padded with unused data |01|00|5e|00|00|02|b0|75|4d|10|f3|53|.
- |08|00| must be present in the header to signify to Wireshark that the next bytes from the packet via the Firewall subsystem are in an IP packet.

```
debug
    security
        capture
            custom-format
                header "+----------+---------------+----------
+\n%hh:%mm:%ss,%iii,%uuu   ETHER\n|0   |01|00|5e|00|00|02|b0|75|4d|10|f3|53|08|00|"
                no audit-report
                no packet-decode
                packet-hex-dump delimiter |
                footer "\n"
            exit
            from zone "1"
            destination console
            format custom
            start
        exit
```

```
    exit
exit
```

audit-report

Syntax [**no**] **audit-report**

Context debug>security>capture>custom-format

Description This command specifies whether to include or remove the audit report from the log.

An audit report is the portion of the header that contains information pertaining to zones and the source interface, as illustrated in the example below.

```
7 09/12/2017 21:36:30.1Jt2345000 UTC SECURITY:Capture Base IF:if_ixl
Outbound : 1
Inbound  : <None>
Session  : None
Report   : NoRuleMatched
Action   : REJECT
IP header -
  ver:4  hlen:20  tos:0x00  len:248  hxsum:0x50f0
  id:0x0000 frag:000 (offset:0)
 10.1.1.2->10.10.10.3  proto:UDP
UDP header     :
   sport :63 dport :63 len :228 xsum: 0xce2f
```

footer

Syntax **footer** *footer-string*
no footer

Context debug>security>capture>custom-format

Description This command defines a custom footer for the log.

Default n/a

Parameters *footer-string* — specifies the format of the footer string, 256 characters maximum

For example, using the footer string “%LLL-%YYYY%MMM%DD -%-AAAAAA” results in the following data: “001-2015Oct30 - PASS “.

Values

Conversion Character Support:
—Use prefix '%'
—Use “-” for left justification
—Repeat character to force field size

Date and Time:	Y: Year (for example, 2017) M: Month M/MM—numeric MMM+—name (for example, Feb)) D: Day of the month h: Hour m: Minute s: Seconds i: Milliseconds u: Microseconds z: Time zone (for example, UTC)
Packet Information:	A: Packet action S: Source interface name R: Source router/VPRN name O: Outgoing zone name I: Incoming zone name F: Session/flow identifier
Log/Capture Information:	L: Log event number
Escape Character Support:	—Use prefix “\” n: New line

header

Syntax [**no**] **header** *header-string*

Context debug>security>capture>custom-format

Description This command defines a custom header for the log.

Default n/a

Parameters *header-string* — specifies the format of the header string, 256 characters maximum

For example, using the header string “%LLL-%YYYY%MMM%DD -%-AAAAAA” results in the following data: “001-2015Oct30 - PASS “.

Values

Conversion Character Support:	—Use prefix '%' —Use “-” for left justification —Repeat character to force field size

Date and Time:	Y: Year (for example, 2017) M: Month M/MM—numeric MMM+—name (for example, Feb)) D: Day of the month h: Hour m: Minute s: Seconds i: Milliseconds u: Microseconds z: Time zone (for example, UTC)
Packet Information:	A: Packet action S: Source interface name R: Source router/VPRN name O: Outgoing zone name I: Incoming zone name F: Session/flow identifier
Log/Capture Information:	L: Log event number
Escape Character Support:	—Use prefix “\” n: New line

packet-decode

Syntax [**no**] **packet-decode**

Context debug>security>capture>custom-format

Description This command specifies to include or remove packet decoding in the log.

packet-hex-dump

Syntax [**no**] **packet-hex-dump** [**delimiter** *ascii-character*] [**byte-count**] [**ascii-decode**]

Context debug>security>capture>custom-format

Description This command specifies to include or remove packet hex dumping in the log.

Default n/a

Parameters **delimiter** — specifies a character that appears between bytes in the hexadecimal dump

ascii-character — specifies the ASCII character used to delimit bytes in the hexadecimal dump

byte-count — specifies to include the byte count column

ascii-decode — specifies to include the ascii decode column

destination

Syntax **destination** {**memory** | **console**}

Context debug>security>capture

Description This command specifies the destination for captured packets.

Parameters **memory** — the captured packets will be stored in the debug security log, which can be viewed using the **show>security>capture** command

console — the captured packets will appear on the console

format

Syntax **format** {**decode** | **raw** | **custom**}

Context debug>security>capture

Description This command specifies the format in which packets are displayed in the debug security log when captured packets are sent to memory.

Default decode

Parameters **decode** — the debug security log displays the packet IP header and relevant Layer 4 headers

raw — the debug security log displays the raw packet in hexadecimal format

custom — the debug security log displays data based on user input in the custom-format commands.

from

Syntax **from** {*zone-id* | *name*}
no from

Context debug>security>capture

Description This command specifies the security zone from which to capture packets. This command is mandatory for enabling the capturing process.

Parameters *name* — the name of the zone, which has already been defined.

zone-id — the zone ID number, from 1 to 65535

match

Syntax [**no**] **match** [**pass** | **reject**] [**protocol** *protocol-id*] [**src-ip** *src-ip-address/mask*] [**src-port** *src-port*] [**dst-ip** *dst-ip-address/mask*] [**dst-port** *dst-port*] [**size** *packet-size*] [**tcp-handshake**]

Context debug>security>capture

Description This command configures match criteria for selecting packets to be captured from the specified security zone. Up to 10 match criteria can be specified for each packet-capture log. If no criteria are specified, all packets are captured.

The **pass** and **reject** parameters specify to match the action code along with a match criteria for capturing packets. If no action is specified, all packets are displayed.

The **tcp-handshake** criterion applies to strict TCP sessions and only displays TCP session establishment and close operations; it does not display the data frames that pass through the session.

Parameters **pass** — specifies to display packets that match the pass action

reject — specifies to display packets that match the reject action

protocol-id — specifies the protocol name or protocol number on which to match criteria

protocol-name — specifies to match on the protocol name

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip, * - udp/tcp wildcard

protocol-number — specifies to match on the protocol number, from 0 to 255 (see Table 78)

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

src-ip-address/mask — specifies to match on the source IP address

src-port — specifies to match on the source port

dst-ip-address/mask — specifies to match on the destination IP address

dst-port — specifies to match on the destination port

packet-size — specifies to match on the packet size, 1 to 65535

tcp-handshake — specifies to match on the TCP three-way handshake

start

Syntax **start** [**count** *packets*]

Context debug>security>capture

Description This command begins the packet capturing process for the specified security zone. The packet capture process is continuous. When the log reaches 1024 entries, the oldest entry in the log is overwritten with a new one. The optional **count** parameter specifies the number of packets that will be captured before the oldest entry in the log is overwritten with a new one.

Note: The contents of the packet-capture log are cleared each time the **start** command is issued.

Parameters **count** — the number of packets that will be captured before the oldest entry is overwritten

packets — 1 to 1024

stop

Syntax **stop**

Context debug>security>capture

Description This command stops the packet capturing process for the specified security zone.

4 VRRP

This chapter provides information about configuring Virtual Router Redundancy Protocol (VRRP) parameters.

Topics in this chapter include:

4.1 VRRP Overview

Virtual Router Redundancy Protocol (VRRP) is a method of implementing a redundant IP interface shared between two or more routers on a common LAN segment, allowing a group of routers to function as one virtual router. If the IP interface of the virtual router is specified as a default gateway on hosts directly attached to the LAN, the routers sharing the IP interface by participating in VRRP as part of the virtual router instance will prevent a single point of failure by ensuring access to this gateway address. VRRP can be implemented on IES and VPRN service interfaces. VRRPv3 can also be implemented on IES and VPRN service interfaces, including r-VPLS interfaces for both IES and VPRN.

The 7705 SAR supports VRRPv3 for IPv4 and IPv6 as described in RFC 5798. Within a VRRP router, the virtual routers in each of the IPv4 and IPv6 address families are in separate domains and do not overlap.

Note: RFC 5798 uses the term “master” state to denote the virtual router that is currently acting as the active forwarding router for the VRRP instance.

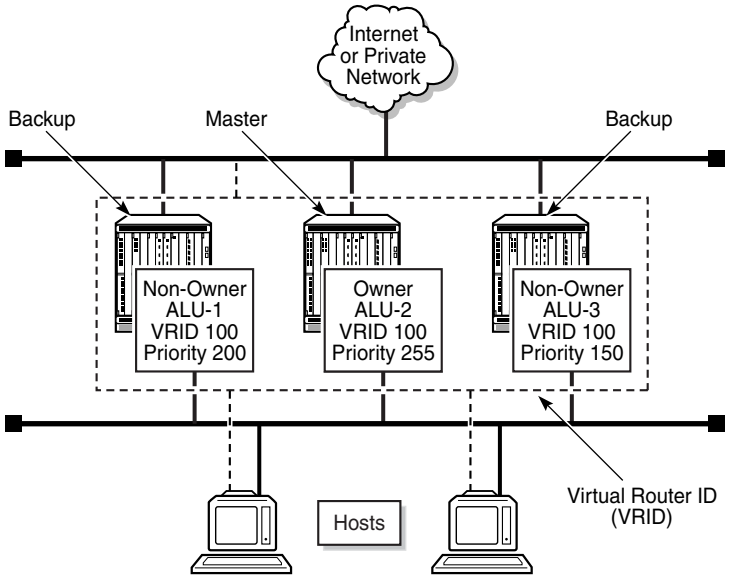
With VRRP, one router is designated as the virtual router in master state (active router) and the other routers in the group act as backups. The active router forwards all packets sent to the virtual IP address. If the router fails, an election process begins and the backup router configured with the highest acceptable priority becomes the active virtual router. The new active router assumes the packet forwarding for the local hosts.

VRRP is supported on Ethernet adapter cards only.

Note: This section describes the configuration parameters of VRRP on IES and VPRN service interfaces as well as configuration parameters of VRRP policies. CLI command descriptions for VRRP policies are given in VRRP Command Reference. For CLI command descriptions related to IES and VPRN service interfaces, refer to the 7705 SAR Services Guide.

Figure 10 shows an example of a VRRP configuration.

Figure 10 **VRRP Master/Backup Configuration**



4.2 VRRP Components

VRRP consists of the following components:

- Virtual Router
- IP Address Owner
- Primary Address
- Virtual Router in Master State
- Virtual Router Backup
- Owner and Non-owner VRRP
- Configurable Parameters

4.2.1 Virtual Router

A virtual router is a logical entity managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a virtual router ID (VRID) and one or more IP addresses across a common LAN. A VRRP router can back up one or more virtual routers.

The purpose of supporting multiple IP addresses within a single virtual router is for multi-netting. This is a common mechanism that allows multiple local subnet attachments on a single routing interface.

Up to four virtual routers are configurable on a single 7705 SAR interface. The virtual routers must be in the same subnet. Each virtual router has its own VRID, state machine, and messaging instance.

4.2.2 IP Address Owner

VRRP can be configured on a router in either owner or non-owner mode. The owner is the VRRP router that has the virtual router's IP addresses as real interface addresses. This is the router that responds to packets addressed to one of the IP addresses for items such as ICMP pings and TCP connections. All other virtual router instances participating in this message domain must have the same VRID configured and cannot be configured as owner.

4.2.3 Primary Address

A primary address is an IP address selected from the set of real interface addresses. For IPv4, VRRP advertisements are always sent using the primary IPv4 address as the source of the IPv4 packet. For IPv6, the link-local address of the interface over which the packet is transmitted is used.

A 7705 SAR IP interface must always have a primary IP address assigned for VRRP to be active on the interface. The 7705 SAR supports primary addresses and multi-netting on the IP interface. The virtual router VRID primary IP address is always the same as the primary address on the IP interface.

4.2.4 Virtual Router in Master State

A physical router that is participating in VRRP and which controls the IP addresses associated with the virtual router is considered to be in the master state, is the active router for the VRRP instance, and is responsible for forwarding packets sent to the VRRP IP addresses. This virtual router is the IP address owner as long as the router is available.

An election process provides dynamic failover of the forwarding responsibility to the backup router if the master becomes unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first-hop router by end hosts. VRRP enables a higher-availability default path without requiring configuration of dynamic routing or router discovery protocols on every end host.

If the master is unavailable, each virtual router backup with the same VRID compares its configured priority values with the other backup routers to determine the master role. Priority values are set with the **priority** command. In case of a tie, the virtual router backup with the highest primary IP address becomes the master.

The **preempt** parameter is supported and can be set to false (disabled) to prevent a backup router that has a higher priority value from becoming master if an existing non-owner virtual router is the current master. Disabling Preemption ensures that the preferred router will regain its master status when service restoration occurs and it goes back on line. Preemption can be enabled or disabled.

While operating as the master, a virtual router routes and originates all IP packets into the LAN using the physical MAC address for the IP interface as the Layer 2 source MAC address, not the VRID MAC address. ARP packets also use the parent IP interface MAC address as the Layer 2 source MAC address while inserting the virtual router MAC address in the appropriate hardware address field. VRRP messages are the only packets transmitted using the virtual router MAC address as the Layer 2 source MAC address.

4.2.5 Virtual Router Backup

A new virtual router master is selected from the set of VRRP virtual router backups available to assume forwarding responsibility for a virtual router if the current master fails.

4.2.6 Owner and Non-owner VRRP

Only one virtual router in the domain is configured as owner. The owner has the same real IP address as the virtual router address and is responsible for forwarding packets sent to this IP address. The owner assumes the role of the virtual router master. All virtual router instances participating in this message domain must have the same VRID configured.

VRRP on a 7705 SAR router can be configured to allow non-owners to respond to ICMP echo requests if they become the virtual router in master state for the VRRP instance. Telnet and other connection-oriented protocols can be configured for master. However, the individual application conversations (connections) do not survive a VRRP failover. A non-owner VRRP router operating as a backup does not respond to any packets addressed to any of the virtual router IP addresses.

The most important parameter defined on a non-owner virtual router instance is the **priority** parameter. The priority defines the order in which a virtual router is selected as master in the master election process. The priority value and the preempt mode determine which virtual router becomes the virtual router master. In case of tied priority levels, the primary IP address determines which router becomes the master. See Priority and Preempt Mode for details on these parameters.

4.2.7 Configurable Parameters

In addition to virtual IP addresses, to facilitate configuration of a virtual router on 7705 SAR routers, the parameters listed in Table 66 can be defined in owner and non-owner configurations.

Table 66 **Owner and Non-owner Virtual Router Parameters**

Parameter	Owner Configuration	Non-owner Configuration
VRID	✓	✓
Message Interval and Master Inheritance	✓	✓
VRRP Message Authentication (IPv4 only)	✓	✓
Virtual MAC Address	✓	✓
BFD-Enable	✓	✓
Initial Delay Timer	✓	✓
Priority		✓
IP Addresses		✓
Master Down Interval [1]		✓
Skew Time [1]		✓
Preempt Mode		✓
VRRP Advertisement Message IP Address List Verification		✓
IPv6 Virtual Router Instance Operationally Up		✓
Policies		✓

Note:

1. Master down interval and skew time are not configured directly. They are calculated from the configured value of the message interval.

4.2.7.1 VRID

The VRID must be configured with the same value on each virtual router associated with the virtual IP address or IP addresses. The VRID is placed in all VRRP advertisement messages sent by each virtual router.

4.2.7.2 Priority

The priority value affects the interaction between all virtual routers with the same VRID participating on the same LAN. The priority value is used during the election process to determine which backup router (or non-owner) will assume the role of master. The priority value can only be configured if the defined IP address on the IP interface is different from the virtual router IP address, meaning that the virtual router is a non-owner.

If the IP address on the IP interface matches the virtual router IP address (owner mode), the priority value is fixed at 255, the highest value possible. This virtual router member is considered the owner of the virtual router IP address. There can only be one owner of the virtual router IP address for all virtual router members.

Priority value 0 is reserved for VRRP advertisement messages. It is used to tell other virtual routers with the same VRID that this virtual router is no longer acting as master, triggering a new election process. If this happens, each virtual router backup sets its master down timer equal to the skew time value. This shortens the time before one of the virtual router backups becomes master. See Master Down Interval and Skew Time for details.

The current virtual router master must transmit a VRRP advertisement message immediately upon receipt of a VRRP message with priority set to 0. This prevents another virtual router backup from becoming master for a short period of time.

Non-owner virtual routers can be configured with a priority of 254 through 1. The default value is 100. It is possible for multiple non-owners to have the same priority value. If a tie is encountered during an election, the router with the highest IP address will win the election.

The priority is also used to determine when to preempt the existing master. If the preempt mode value is true (preempt enabled), VRRP advertisement messages from lower-priority masters are discarded, causing the master down timer to expire and the higher-priority backup router to transition to the master state.

The priority value also dictates the skew time added to the master timeout period. See Skew Time for details.

4.2.7.3 IP Addresses

Each virtual router with the same VRID is defined with the same set of IP addresses. These are the IP addresses used by hosts on the LAN as gateway addresses. Multi-netting supports eight IP addresses on the IP interface.

4.2.7.4 Message Interval and Master Inheritance

Each virtual router is configured with a message interval for each VRID within which it participates. This parameter must be set to the same value for every virtual router within a VRID.

Configuring the message interval value can be done in three ways: using only the milliseconds value, using only the seconds value, or using a combination of the two values, as indicated by the CLI command **message interval** {[*seconds*] [**milliseconds** *milliseconds*]}. Table 67 shows the ranges for each way of configuring the message interval.

Table 67 **Message Interval Configuration Ranges**

Configuration	IPv4	IPv6
Using milliseconds value only	100 to 900 ms	10 to 990 ms
Using seconds value only	1 to 255 s	1 to 40 s
Using combination milliseconds and seconds values	1 s 100 ms to 255 s 900 ms (1.1 s to 255.9 s)	1 s 10 ms to 40s 990 ms (1.01 s to 40.99 s)
Default setting	1 s	1 s

The message interval field in every received VRRP advertisement message must match the locally configured message interval. If a mismatch occurs, then—depending on the inherit parameter configuration (**master-int-inherit** command is enabled)—the current message interval setting of the master can be used to operationally override the locally configured message interval setting. If the current master changes, the new master setting is used. If the local virtual router becomes master, the locally configured message interval is enforced.

If a VRRP advertisement message is received with a message interval set to a value different from the local value and the inherit parameter is disabled, the message is discarded without processing.

The virtual router master uses the message interval as a timer, specifying when to send the next VRRP advertisement message. Each virtual router backup uses the message interval (with the configured local priority) to derive the master down timer value.

VRRP advertisement messages that are fragmented or contain IP options (IPv4) or extension headers (IPv6) require a longer configured message interval.

The virtual router instance can inherit the master VRRP router's message interval timer, which is used by backup routers to calculate the master down timer.

The inheritance is only configurable in the non-owner context. It is used to allow the current virtual router master to dictate the master down timer for all virtual router backups.

Note: A message interval is the same as an advertisement interval.

4.2.7.5 Master Down Interval

The master down interval is the time that the master router can be operationally down before a backup router takes over. The master down interval is a calculated value used to specify the master down timer. If the master down timer expires, the backup virtual router enters the master state. To calculate the master down interval, the virtual router uses the following formula:

Master Down Interval = (3 × Operational Message Interval) + Skew Time

The operational message interval is dependent upon the state of the inherit parameter, as follows. See Message Interval and Master Inheritance for details.

- If the inherit parameter is enabled, the operational message interval is derived from the current master's message interval field in the VRRP advertisement message.
- If the inherit parameter is disabled, the operational message interval must be equal to the locally configured message interval.

The master down timer is only operational if the local virtual router is operating in backup mode.

4.2.7.6 Skew Time

The skew time is used to add a time period to the master down interval. Skew time is not a configurable parameter. It is derived from the current local priority of the virtual router. To calculate the skew time (as per RFC 5798), the virtual router uses the following formula:

Skew Time = (((256 – priority) × Master_Adver_Interval) / 256) centiseconds

A higher priority value means a smaller skew time. This means that a virtual router with a higher priority will transition to the master router more quickly than a virtual router with a lower priority.

4.2.7.7 Preempt Mode

Preempt mode is a configured true or false value that controls whether a virtual router backup with a higher priority preempts a lower-priority master. Preempt mode cannot be set to false on the owner virtual router.The IP address owner always becomes master if available. The default value for preempt mode is true.

If the preempt mode is true (enabled), the advertised priority from the incoming VRRP advertisement message from the current master is compared to the local configured priority, with the following results.

- If the local priority is higher than the received priority, the received VRRP advertisement message is discarded. This results in the eventual expiration of the master down timer, causing the backup router to transition to the master state.
- If the received priority is equal to the local priority, the message is not discarded and the current master is not replaced. The received primary IP address is not part of the decision to preempt and is not used as a tiebreaker if the received and local priorities are equal.

If the preempt mode is false (disabled), the virtual router only becomes master if the master down timer expires before a VRRP advertisement message is received from another virtual router.

4.2.7.8 VRRP Message Authentication (IPv4 only)

VRRP message authentication uses a simple text password authentication key to generate master VRRP advertisement messages and validate received VRRP advertisement messages.

If the **authentication-key** command is re-executed with a different password key defined, the new key will be used immediately. If a **no authentication-key** command is executed, the password authentication key is restored to the default value. The **authentication-key** command may be executed at any time.

VRRP message authentication is applicable to IPv4 VRRP only.

4.2.7.8.1 Authentication Failure

Any received VRRP advertisement message that fails authentication is silently discarded with an invalid authentication counter incremented for the ingress virtual router instance.

4.2.7.9 Virtual MAC Address

The MAC address can be used instead of an IP address in ARP responses if the virtual router instance is master. The MAC address configuration must be the same for all virtual routers with the same VRID; otherwise, the result is indeterminate connectivity by the attached IP hosts. All VRRP advertisement messages are transmitted with the IEEE address as the source MAC address.

4.2.7.10 BFD-Enable

A BFD session can be used to provide a heartbeat mechanism for a VRRP instance. Only one BFD session can be assigned to a VRRP instance, but multiple VRRP instances can use the same BFD session.

BFD controls the state of the associated interface. By enabling BFD on a protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node.

4.2.7.11 Initial Delay Timer

A VRRP initialization delay timer can be configured in the range of 1 to 65535 seconds.

4.2.7.12 VRRP Advertisement Message IP Address List Verification

VRRP messages contain an IP address count field that indicates the number of IP addresses listed in the sequential IP address fields at the end of the message. The 7705 SAR implementation always logs mismatching events. The decision on where and whether to forward the generated messages depends on the configuration of the event manager. The log message is generated by network management and is not the same as the VRRP message.

Each virtual router instance maintains a record of the mismatch states associated with each source IP address in the VRRP master table. If the state changes, a mismatch log message is generated indicating the source IP address within the message, the mismatch or match event, and the time of the event.

If secondary IP addresses are used, the message contains multiple IP addresses, which must match the IP addresses on the virtual router instance. Owner and non-owner virtual router instances have the supported IP addresses explicitly defined, making mismatched supported IP addresses within the interconnected virtual router instances a configuring issue.

4.2.7.13 IPv6 Virtual Router Instance Operationally Up

When the IPv6 virtual router is properly configured with a minimum of one link-local backup address, the parent interface's router advertisement must be configured to use the virtual MAC address in order for the virtual router to be considered operationally up.

4.2.7.14 Policies

Policies can be configured to control VRRP priority with the virtual router instance. A policy can be associated with more than one virtual router instance. Policies can only be configured in the non-owner VRRP context. See VRRP Priority Control Policies for details.

4.3 VRRP Priority Control Policies

VRRP supports control policies to manipulate virtual router participation in the VRRP master election process and the state of the master. The local priority value for the virtual router instance is used to control the election process and master state.

This section contains information on the following topics:

- VRRP Policy Constraints
- VRRP Base Priority
- VRRP Priority Control Policy In-use Priority
- VRRP Priority Control Policy Priority Events

4.3.1 VRRP Policy Constraints

Priority control policies can only be applied to non-owner VRRP virtual router instances. Owner VRRP virtual routers cannot be controlled by a priority control policy because they must have a priority value of 255 that cannot be lowered. Only one VRRP priority control policy can be applied to a non-owner virtual router instance.

Multiple VRRP virtual router instances can be associated with the same IP interface, allowing multiple priority control policies to be associated with the IP interface.

An applied VRRP priority control policy only affects the in-use priority on the virtual router instance if the preempt mode has been enabled. A virtual router instance with preempt mode disabled always uses the base priority as the in-use priority, ignoring any configured priority control policy.

4.3.2 VRRP Base Priority

The base priority is the starting priority for the VRRP instance and is set using the service interface **priority** command. The actual in-use priority for the VRRP instance is derived from the base priority and an optional VRRP priority control policy that modifies the base priority.

VRRP priority control policies are used to either override or adjust the base priority value depending on events or conditions within the chassis.

Non-owner virtual router instances must have a base priority value between 1 and 254. The value 0 is reserved to indicate master termination in VRRP advertisement messages. The value 255 is reserved for the VRRP owner. The default base priority for non-owner virtual router instances is 100.

4.3.3 VRRP Priority Control Policy In-use Priority

A VRRP priority control policy enforces an overall minimum value that the policy can impose upon the VRRP virtual router instance base priority. This value provides a lower limit to the delta priority event manipulation of the base priority.

A delta priority event is a conditional event defined in the priority control policy that subtracts a given amount from the current base priority for all VRRP virtual router instances to which the policy is applied. Multiple delta priority events can apply simultaneously, creating a dynamic priority value. The base priority for the instance, minus the sum of the delta values, sets the actual priority in-use value.

An explicit priority event is a conditional event defined in the priority control policy that explicitly defines the in-use priority for the virtual router instance. The explicitly defined values are not affected by the delta in-use priority limit. If multiple explicit priority events happen simultaneously, the lowest value is used for the in-use priority. The configured base priority is not a factor in explicit priority overrides of the in-use priority.

The allowed range of the delta in-use priority limit is 1 to 254. The default is 1, which prevents the delta priority events from operationally disabling the virtual router instance.

4.3.4 VRRP Priority Control Policy Priority Events

This section contains information on the following topics:

- Priority Event Hold-set Timers
- Port Down Priority Event
- LAG Port Down Priority Event
- Host Unreachable Priority Event
- Route Unknown Priority Event

The main function of a VRRP priority control policy is to define conditions or events that impact the ability of the system to communicate with outside hosts or portions of the network. If one or more of these events are true, the base priority on the virtual router instance is either overwritten with an explicit value, or a sum of delta priorities is subtracted from the base priority. The result is the in-use priority for the virtual router instance. Any priority event can be configured as an explicit event or a delta event.

Outside hosts are the network entities that generate the IP user traffic. VRRP communication occurs between the routers on the subnet that are using VRRP. The availability of routes and/or hosts can influence the priority of a VRRP router, making the priority variable. If a backup router loses the ability to route to some destinations, its VRRP priority is reduced, making it less desirable as a backup router in case the master fails.

Explicit events override all delta events. If multiple explicit events occur, the event with the lowest priority value is assigned to the in-use priority. As events clear, the in-use priority is re-evaluated accordingly and adjusted dynamically.

Delta priority events also have priority values. If no explicit events have occurred within the policy, the sum of the occurring delta events priorities is subtracted from the base priority of each virtual router instance. If the result is lower than the delta in-use priority limit, the delta in-use priority limit is used as the in-use priority for the virtual router instance. Otherwise, the in-use priority is set to the base priority less the sum of the delta events.

Each event generates a VRRP priority event message indicating the policy ID, the event type, the priority type (delta or explicit) and the event priority value. Another log message is generated if the event is no longer true, indicating that the event has been cleared.

4.3.4.1 Priority Event Hold-set Timers

Hold-set timers are used to dampen the effect of a flapping event. A flapping event occurs when an event continually transitions between clear and set. The hold-set timer prevents a set event from transitioning to the cleared state until it expires.

Each time an event transitions between cleared and set, the timer begins to count down to 0. If the timer reaches 0, the event is allowed to enter the cleared state once more. Entering the cleared state is always dependent on the object controlling the event conforming to the requirements defined in the event itself. It is possible, on some event types, to have another set action reset the hold-set timer. This extends the amount of time that must expire before entering the cleared state.

4.3.4.2 Port Down Priority Event

The port down priority event is associated with a physical port. The port operational state is evaluated to determine a port down priority event or event clear.

If the port operational state is up, the port down priority event is considered false (or cleared). If the port operational state is down, the port down priority event is considered true (or set).

4.3.4.3 LAG Port Down Priority Event

The LAG port down priority event is associated with a LAG. The event monitors the operational state of each port in the specified LAG.

When one or more of the ports enter the operationally down state, the event is considered to be set. When all the ports enter the operationally up state, the event is considered to be clear. As ports enter the operational up state, any previous set threshold that represents more down ports is considered cleared, while the event is considered to be set.

4.3.4.4 Host Unreachable Priority Event

The host unreachable priority event creates a continuous ping task that is used to test connectivity to a remote host. For the ping to be successful, the path to the remote host, and the remote host itself, must be capable and configured to accept ICMP echo requests and replies.

The ping task is controlled by interval and size parameters that define how often the ICMP request messages are transmitted and the size of each message. A historical missing reply parameter defines if the ping destination is considered unreachable.

If the host is unreachable, the host unreachable priority event is considered true (or set). If the host is reachable, the host unreachable priority event is considered false (or cleared).

4.3.4.5 Route Unknown Priority Event

The route unknown priority event defines a task that monitors the existence of a given route prefix in the routing table of the system.

The route monitoring task can be constrained by a condition that allows a prefix that is less specific than the defined prefix to be considered as a match. The source protocol can be defined to indicate the protocol the installed route must be populated from. To further define match criteria when multiple instances of the route prefix exist, an optional next-hop parameter can be defined.

If a route prefix exists within the active route table that matches the defined match criteria, the route unknown priority event is considered false (or cleared). If a route prefix does not exist within the active route table that matches the defined criteria, the route unknown priority event is considered true (or set).

4.4 VRRP Non-owner Accessibility

Although only VRRP owners can respond to ping and other management-oriented protocols directed to the VRID IP addresses, the 7705 SAR allows an override of this restraint on a per-VRRP virtual router instance basis.

This section contains information on the following topics:

- Non-owner Access Ping Reply
- Non-owner Access Telnet
- Non-owner Access SSH

4.4.1 Non-owner Access Ping Reply

If non-owner access ping reply is enabled on a virtual router instance, ICMP echo request messages destined for the non-owner virtual router instance IP addresses are not discarded at the IP interface if the virtual router is operating in master mode. ICMP echo request messages are always discarded in backup mode.

If non-owner access ping reply is disabled on a virtual router instance, ICMP echo request messages destined for the non-owner virtual router instance IP addresses are silently discarded in both the master and backup modes.

4.4.2 Non-owner Access Telnet

If non-owner access Telnet is enabled on a virtual router instance, authorized Telnet sessions can be established that are destined for the virtual router instance IP addresses if the virtual router is operating in master mode. Telnet sessions are always discarded at the IP interface if destined for a virtual router IP address on a virtual router operating in backup mode. Enabling non-owner access Telnet does not guarantee Telnet access; proper management and security features must be enabled to allow Telnet on this interface and possibly from the given source IP address.

If non-owner access Telnet is disabled on a virtual router instance, Telnet sessions destined for the non-owner virtual router instance IP addresses are silently discarded in both master and backup modes.

4.4.3 Non-owner Access SSH

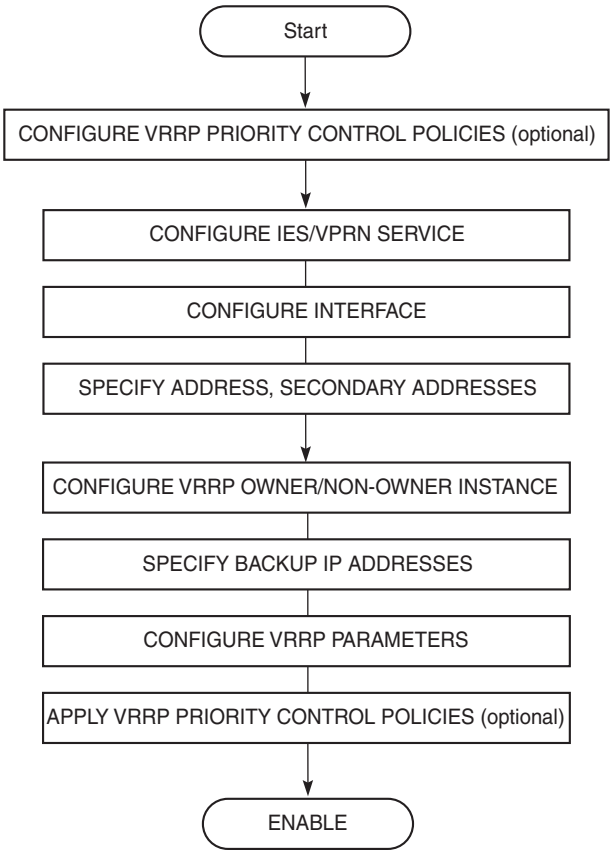
If non-owner access SSH is enabled on a virtual router instance, authorized SSH sessions can be established that are destined for the virtual router instance IP addresses if the virtual router is operating in master mode. SSH sessions are always discarded at the IP interface when destined for a virtual router IP address on a virtual router operating in backup mode. Enabling non-owner access SSH does not guarantee SSH access; proper management and security features must be enabled to allow SSH on this interface and possibly from the given source IP address. SSH is applicable to IPv4 VRRP only.

If non-owner access SSH is disabled on a virtual router instance, SSH sessions destined for the non-owner virtual router instance IP addresses are silently discarded in both master and backup modes.

4.5 VRRP Configuration Process Overview

Figure 11 displays the process to provision VRRP parameters.

Figure 11 **VRRP Configuration**



4.6 Configuration Notes

The following are VRRP configuration guidelines and caveats:

- creating and applying VRRP policies are optional
- **backup** command:
  - the virtual backup IP addresses must be on the same subnet. The backup addresses explicitly define which IP addresses are in the VRRP message IP address list.
  - in owner mode, the backup IP address must be identical to one of the interface IP addresses
  - for IPv6, one of the backup addresses configured must be the link-local address of the owner VRRP instance

4.7 Configuring VRRP with CLI

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

- VRRP Configuration Overview
- Basic VRRP Configurations
- Common Configuration Tasks
- Configuring IES or VPRN VRRP Parameters
- VRRP Management Tasks

4.8 VRRP Configuration Overview

Configuring VRRP policies and instances on service interfaces is optional. The basic owner and non-owner VRRP configurations on an IES or VPRN service interface must specify the **backup** *ip-address* parameter.

VRRP helps eliminate the single point of failure in a routed environment by using virtual router IP addresses shared between two or more routers connecting the common domain. VRRP provides dynamic failover of the forwarding responsibility to the backup router if the master becomes unavailable.

The VRRP implementation allows one master per IP subnet. All other VRRP instances in the same domain must be in backup mode.

4.8.1 Preconfiguration Requirements

VRRP policies:

- VRRP policies must be configured before they can be applied to an IES or VPRN VRRP instance. VRRP policies are configured in the **config>vrrp** context.
- If the policy will be associated with a VPRN VRRP interface, the VRRP policy configuration must include the VPRN service ID to which the policy applies; otherwise, when the user attempts to associate the policy with the VPRN VRRP interface, an error message indicating that the policy ID does not exist will be returned.

Configuring VRRP on an IES or VPRN service interface:

- the service customer account must be created prior to configuring an IES or VPRN VRRP instance
- the interface address must be specified in both the owner and non-owner IES or VPRN instances

4.9 Basic VRRP Configurations

VRRP parameters are configured in the following contexts:

- VRRP Policy
- VRRP IES or VPRN Service Parameters

4.9.1 VRRP Policy

Configuring and applying VRRP policies is optional. There are no default VRRP policies. Each policy must be explicitly defined. A VRRP configuration must include the following:

- policy ID
- service ID (mandatory for VPRN service only)
- at least one of the following priority events:
  - port down
  - LAG port down
  - host unreachable
  - route unknown

Policies can only be applied to non-owner VRRP virtual router instances.

The following example displays a configuration of an IES VRRP policy.

```
config>vrrp>policy# info
----------------------------------------------
    delta-in-use-limit 50
    priority-event
        port-down 4/1/2
            hold-set 43200
            priority 100 delta
        exit
        port-down 4/1/3
            priority 200 explicit
        exit
        lag-port-down 1
            number-down 3
                priority 50 explicit
            exit
        exit
        host-unreachable 10.10.24.4
            drop-count 25
        exit
        route-unknown 10.10.0.0/32
```

```
            priority 50 delta
            protocol bgp
        exit
    exit
-----------------------------------------------
```

The following example displays a configuration of a VPRN VRRP policy, with service ID 10 specified.

```
config>vrrp>policy 1 context 10# info
-----------------------------------------------
....
        priority event port-down 1/1/1
            priority 200 explicit
        exit
        lag-port-down 1
            number-down 3
                priority 50 explicit
            exit
        exit
      exit
    exit
-----------------------------------------------
```

4.9.2 VRRP IES or VPRN Service Parameters

VRRP parameters are configured within an IES or VPRN service with one of two contexts, owner or non-owner. The status is specified when the VRRP configuration is created. When configured as owner, the virtual router instance has the same real IP addresses as the virtual backup IP addresses. All other virtual router instances participating in this message domain must have the same VRID configured and cannot be configured as owner.

Note: VRRP service parameter configuration is the same for both VPRN and IES services.

For IPv4 and IPv6, up to two VRRP instances (VRIDs) can be configured on an IES or VPRN service interface. IPv4 can back up a maximum of eight addresses per VRRP instance (one primary and seven secondary). IPv6 can back up a maximum of four addresses (one primary and three secondary).

VRRP parameters configured within an IES or VPRN service must include the following:

- VRID
- virtual backup IP addresses

The following example displays a configuration of IES service owner and non-owner VRRP configurations.

```
config>service>ies# info
----------------------------------------------
interface "tuesday" create
   address 10.10.36.2/8
   sap 7/1/1:100 create
   vrrp 19 owner
      backup 10.10.36.7
      authentication-key "testabc"
   exit
exit
interface "testing" create
   address 10.10.10.16/8
   sap 1/1/55:0 create
   vrrp 12
      backup 10.10.10.15
      policy 1
      authentication-key "testabc"
   exit
exit
   no shutdown
----------------------------------------------
config>service>ies#
```

4.9.2.1 Configuring IES or VPRN VRRP for IPv6

The following output shows an IES VRRP for IPV6 configuration example.

```
config>service>ies# info
----------------------------------------------
    description "VLAN 921 for DSC-101 Application"
    interface "DSC-101-Application" create
        address 10.152.2.220/8
        vrrp 217
            backup 10.152.2.222
            priority 254
            ping-reply
        exit
        ipv6
            address 2001:db8:a::123/64
            link-local-address 2001:db8:a::222 preferred
            vrrp 219
                backup 2001:db8:a::122
                priority 254
                ping-reply
            exit
        exit
        sap 1/1/4 create
            description "sap-10-192.168.0.1"
        exit
    exit
    no shutdown
----------------------------------------------
```

4.10 Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure VRRP and lists the CLI commands.

VRRP parameters are defined under a service interface context. An IP address must be assigned to each IP interface. Only one primary IP address can be associated with an IP interface but several secondary IP addresses can be associated.

Owner and non-owner configurations must include the following parameters:

- all participating routers in a VRRP instance must be configured with the same VRID
- all participating non-owner routers can specify up to eight backup IP addresses (that is, the IP addresses that the master is representing). The owner configuration must include at least one backup IP address.
- for IPv6, one of the backup addresses configured must be the link-local address of the owner VRRP instance

Owner and non-owner configurations can also include the following optional commands:

- authentication-key (IPv4 only)
- MAC
- message-interval

In addition to the common parameters, the following non-owner commands can be configured:

- master-int-inherit
- priority
- bfd-enable
- initial delay
- policy
- ping-reply
- preempt
- telnet-reply
- ssh-reply (IPv4 only)
- shutdown

4.11 Configuring IES or VPRN VRRP Parameters

VRRP parameters can be configured on a service interface to provide virtual default router support that allows traffic to be routed without relying on a single router in case of failure. VRRP can be configured in the following ways:

- Configuring VRRP on Subnets
- Owner VRRP
- Non-owner VRRP

4.11.1 Configuring VRRP on Subnets

If you have multiple subnets configured on an IES or VPRN service interface, you can configure VRRP on each subnet.

The following displays an IES interface configuration example:

```
config>service>ies# info
#------------------------------------------
...
    interface "test-A" create
       address 192.168.0.0/16
    exit
    interface "testB"
       address 192.168.0.1/16
       secondary 192.168.0.2/16
       secondary 192.168.0.3/16
       secondary 192.168.0.4/16
    exit
    no shutdown
...
#------------------------------------------
```

4.11.2 Owner VRRP

The following displays an owner VRRP configuration example for an IPv4 service interface:

```
config>service>ies# info
#------------------------------------------------
...
    interface “test2” create
        address 192.168.0.0/16
        vrrp 1 owner
            backup 192.168.0.2
```

```
            authentication-key "testabc"
        exit
    exit
...
#-----------------------------------------------
config>service>ies#
```

If a VRRP instance is created as owner, it cannot be changed to the non-owner state. The VRID must be deleted and then recreated without the **owner** keyword to remove IP address ownership.

4.11.3 Non-owner VRRP

The following displays a basic non-owner VRRP configuration example for an IPv4 service interface:

```
config>service>ies# info
#-----------------------------------------------
...
    interface "test2" create
        address 192.168.0.0/16
        sap 1/1/55:0 create
        vrrp 12
            backup 192.168.0.1
            policy 1
            authentication-key "testabc"
            exit
    exit
    no shutdown
...
#-----------------------------------------------
config>service>ies#
```

If a VRRP instance is created as non-owner, it cannot be changed to the owner state. The VRID must be deleted and then recreated with the **owner** keyword to invoke IP address ownership.

4.12 VRRP Management Tasks

This section discusses the following VRRP management tasks:

- Deleting a VRRP Policy
- Deleting VRRP on a Service

4.12.1 Deleting a VRRP Policy

Policies are only applied to non-owner VRRP instances. A VRRP policy cannot be deleted if it is applied to an IES or VPRN service. Each instance in which the policy is applied must be deleted. The following example displays a policy deletion.

Example:

```
config>vrrp
config>vrrp# no policy 1
```

The" Applied" column in the following example displays whether the VRRP policies are applied to an entity. The services using the VRRP policy can be viewed using the specific policy ID in the CLI command (for example, **show>vrrp>policy 1**).

```
#show>vrrp# policy
=====================================================
VRRP Policies
=====================================================
Policy    Current             Current      Current      Delta Applied Svc
Id        Priority & Effect   Explicit     Delta Sum    Limit         Context
-----------------------------------------------------------------------------
1         70   Delta          None         70           1     Yes     None
100       None                None         None         1     No      None
255       None                None         None         1     No      None
-----------------------------------------------------------------------------


#show>vrrp# policy 1
=============================================================================
VRRP Policy 1
=============================================================================
Description     :
Current Priority: 100 Delta           Applied           : Yes
Current Explicit: None                Current Delta Sum : 100
Delta Limit     : 1                   Svc Context       : None
-----------------------------------------------------------------------------
Rtr Id/    Applied To                      VR   Opr  Base In-use Master Is
Svc Id     Interface Name                  Id        Pri  Pri    Pri    Master
-----------------------------------------------------------------------------
800        tuesday                         6    Down 100  1      0      No
-----------------------------------------------------------------------------
Rtr Id/    Applied To                      IPv6 Opr  Base In-use Master Is
Svc Id     Interface Name                  VR-Id     Pri  Pri    Pri    Master
```

```
-------------------------------------------------------------------------------
None
-------------------------------------------------------------------------------
SRRP        Applied To Interface Name        Oper           Base  In-use Master
Id          Rtr Id/Svc Id                    State          Pri   Pri    Pri
-------------------------------------------------------------------------------
None
-------------------------------------------------------------------------------
Priority Control Events
-------------------------------------------------------------------------------
Event Type & ID                 Event Oper State        Hold Set  Priority In
                                                        Remaining &Effect  Use
-------------------------------------------------------------------------------
Port Down 1/2/1                 Set-down                Expired   100 Del  Yes
===============================================================================
#show>vrrp#
```

4.12.2 Deleting VRRP on a Service

The VRID does not need to be shut down to remove the virtual router instance from a service.

The following example displays the commands to delete a VRRP instance in non-owner mode from an IES service:

Example:

```
config>service# ies 10
config>service>ies# interface test
config>service>ies>if# no vrrp 1
config>service>ies>if# exit all
```

4.13 VRRP Command Reference

4.13.1 Command Hierarchies

4.13.1.1 VRRP Priority Control Event Policy Commands

```
config
    — vrrp
        — policy policy-id [context service-id]
        — no policy policy-id
            — delta-in-use-limit limit
            — no delta-in-use-limit
            — description description-string
            — no description
            — [no] priority-event
                — [no] host-unreachable ip-address
                — [no] host-unreachable ipv6-address
                    — drop-count count
                    — no drop-count
                    — hold-clear seconds
                    — no hold-clear
                    — hold-set seconds
                    — no hold-set
                    — interval seconds
                    — no interval
                    — priority priority-level [delta | explicit]
                    — no priority
                    — timeout seconds
                    — no timeout
                — lag-port-down port-id
                — no lag-port-down
                    — hold-clear seconds
                    — no hold-clear
                    — hold-set seconds
                    — no hold-set
                    — number-down number-of-lag-ports-down
                    — no number-down
                        — priority priority-level [delta | explicit]
                        — no priority
                — port-down port-id
                — no port-down
                    — hold-clear seconds
                    — no hold-clear
                    — hold-set seconds
                    — no hold-set
                    — priority priority-level [delta | explicit]
                    — no priority
                — [no] route-unknown ip-prefix/mask
                — [no] route-unknown ipv6-address/prefix-length
                    — hold-clear seconds
                    — no hold-clear
                    — hold-set seconds
                    — no hold-set
                    — less-specific [allow-default]
                    — no less-specific
                    — [no] next-hop ip-address
                    — priority priority-level [delta | explicit]
```

— **no priority**
— **protocol** *protocol*
— **no protocol**

4.13.1.2 VRRP Show Commands

show
— **vrrp**
— **policy** [*policy-id* [**event** *event-type specific-qualifier*]]
— **router**
— **vrrp**
— **instance**
— **instance interface** *interface-name* [**vrid** *virtual-router-id*]
— **instance interface** *interface-name* **vrid** *virtual-router-id* **ipv6**
— **statistics**

4.13.1.3 VRRP Monitor Commands

monitor
— **router**
— **vrrp**
— **instance interface** *interface-name* **vrid** *virtual-router-id* [**ipv6**] [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

4.13.1.4 VRRP Clear Commands

clear
— **router**
— **vrrp**
— **interface** *interface-name* [**vrid** *virtual-router-id*]
— **interface** *interface-name* **vrid** *virtual-router-id* **ipv6**
— **statistics**
— **statistics interface** *interface-name* [**vrid** *virtual-router-id*]
— **statistics interface** *interface-name* **vrid** *virtual-router-id* **ipv6**

4.13.1.5 VRRP Debug Commands

debug
— **router**
— **vrrp**
— [**no**] **events**
— [**no**] **events interface** *ip-int-name* [**vrid** *virtual-router-id*]

- [**no**] **events interface** *ip-int-name* **vrid** *virtual-router-id* **ipv6**
- [**no**] **packets**
- [**no**] **packets interface** *ip-int-name* [**vrid** *virtual-router-id*]
- [**no**] **packets interface** *ip-int-name* **vrid** *virtual-router-id* **ipv6**

4.13.2 Command Descriptions

4.13.2.1 Configuration Commands

- VRRP Priority Control Event Policy Commands
- VRRP Priority Event Commands

4.13.2.1.1 VRRP Priority Control Event Policy Commands

policy

Syntax **policy** *policy-id* [**context** *service-id*]
no policy *policy-id*

Context config>vrrp

Description This command enables the context to configure a VRRP priority control policy that is used to control the VRRP in-use priority based on priority control events. The VRRP priority control policy commands define policy parameters and priority event conditions.

The virtual router instance **priority** command defines the initial or base value to be used by non-owner virtual routers. This value can be modified by assigning a VRRP priority control policy to the virtual router instance. The VRRP priority control policy can override the base priority setting to establish the actual in-use priority of the virtual router instance.

The **policy** command must be created first, before it can be associated with a virtual router instance.

If the policy will be associated with a VPRN VRRP interface, the *service-id* for the VPRN service to which the policy applies must be specified; otherwise, when the user attempts to associate the policy with the VPRN VRRP interface, an error message indicating that the policy ID does not exist will be returned.

Because VRRP priority control policies define conditions and events that must be maintained, they can be resource-intensive. The number of policies is limited to 10 000.

The policy IDs do not have to be consecutive integers. The range of available policy identifiers is from 1 to 9999.

The **no** form of the command deletes the specific policy ID from the system.

The policy ID must be removed first from all virtual router instances before the **no policy** command can be issued. If the policy ID is associated with a virtual router instance, the command fails.

Default n/a

Parameters *policy-id* — specifies the VRRP priority control ID that uniquely identifies this policy from any other VRRP priority control policy defined on the system. Up to 10 000 policies can be defined.

Values 1 to 9999

service-id — specifies the service ID to which the policy applies

Values 1 to 2147483690 or *service-name*

delta-in-use-limit

Syntax **delta-in-use-limit** *limit*
no delta-in-use-limit

Context config>vrrp>policy

Description This command sets a lower limit on the virtual router in-use priority that can be derived from the delta priority control events.

Each VRRP priority ID places limits on the delta priority control events to define the in-use priority of the virtual router instance. Setting this limit prevents the sum of the delta priority events from lowering the in-use priority value of the associated virtual router instances below the configured value.

The limit has no effect on explicit priority control events. Explicit priority control events are controlled by setting the in-use priority to any value between 1 and 254.

Only non-owner virtual router instances can be associated with VRRP priority control policies and their priority control events.

Once the total sum of all delta events is calculated and subtracted from the base priority of the virtual router instance, the result is compared to the **delta-in-use-limit** value. If the result is less than the limit, the **delta-in-use-limit** value is used as the virtual router in-use priority value. If an explicit priority control event overrides the delta priority control events, the **delta-in-use-limit** has no effect.

Setting the limit to a higher value than the default of 1 limits the effect of the delta priority control events on the virtual router instance base priority value. This allows for multiple priority control events while minimizing the overall effect on the in-use priority

Setting the limit to a value equal to or larger than the virtual router instance base priority prevents the delta priority control events from having any effect on the virtual router instance in-use priority value.

Changing the in-use priority limit causes an immediate re-evaluation of the in-use priority values for all virtual router instances associated with this VRRP policy ID based on the current sum of all active delta control policy events.

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

Default 1

Parameters *limit* — specifies the lower limit of the in-use priority, as modified by priority control policies. The limit has the same range as the non-owner virtual router instance *base-priority* parameter. If the result of the total delta priority control events minus the virtual router instance base priority is less than the limit, the *limit* value is used as the virtual router instance in-use priority value.

Values 1 to 254

description

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

Context config>vrrp>policy

Description This command associates a text string with a configuration context to help identify the content in the configuration file.

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

Default n/a

Parameters *description-string* — specifies 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.

4.13.2.1.2 VRRP Priority Event Commands

priority-event

Syntax [**no**] **priority-event**

Context config>vrrp>policy

Description This command enables the context to configure VRRP priority control events used to define criteria to modify the VRRP in-use priority.

A priority control event specifies an object to monitor and the effect on the in-use priority level for an associated virtual router instance.

Up to 32 priority control events can be configured.

The **no** form of this command clears any configured priority events.

host-unreachable

Syntax [**no**] **host-unreachable** *ip-address*
[**no**] **host-unreachable** *ipv6-address*

Context config>vrrp>policy>priority-event

Description This command enables the context to configure a host unreachable priority control event to monitor the ability to receive ICMP echo reply packets from an IP host address.

A host unreachable priority event creates a continuous ICMP echo request (ping) probe to the specified IP address. If a ping fails, the event is considered to be set. If a ping is successful, the event is considered to be cleared.

Up to 32 unique (different IP addresses) host unreachable events can be configured.

The **host-unreachable** command can reference any valid local or remote IP address. The ability to use ARP to find a local IP address or find a remote IP address within a route prefix in the route table is considered part of the monitoring procedure. The host unreachable priority event operational state tracks ARP or route table entries dynamically appearing and disappearing from the system. The operational state of the host unreachable event can be one of the following:

Host Unreachable Operational State	Description
Set – no ARP	No ARP address found for IP address for drop-count consecutive attempts. Only applies when IP address is considered local.

Set – no route	No route exists for IP address for drop-count consecutive attempts. Only applies when IP address is considered remote.
Set – host unreachable	ICMP host unreachable message received for drop-count consecutive attempts
Set – no reply	ICMP echo request timed out for drop-count consecutive attempts
Set – reply received	Last ICMP echo request attempt received an echo reply but historically not able to clear the event
Cleared – no ARP	No ARP address found for IP address – not enough failed attempts to set the event
Cleared – no route	No route exists for IP address – not enough failed attempts to set the event
Cleared – host unreachable	ICMP host unreachable message received – not enough failed attempts to set the event
Cleared – no reply	ICMP echo request timed out – not enough failed attempts to set the event
Cleared – reply received	Event is cleared – last ICMP echo request received an echo reply

Unlike other priority event types, the host unreachable priority event monitors a repetitive task. A historical evaluation is performed on the success rate of receiving ICMP echo reply messages. The operational state takes the cleared and set orientation from the historical success rate. The informational portion of the operational state is derived from the result of the last attempt. It is possible for the previous attempt to fail while the operational state is still cleared due to an insufficient number of failures to cause it to become set. It is also possible for the state to be set while the previous attempt was successful.

When an event transitions from clear to set, the set is processed immediately and must be reflected in the associated virtual router instance in-use priority value. As the event transitions from clear to set, a hold-set timer is started with the value configured by the event's **hold-set** command. This timer prevents the event from clearing until it expires, damping the effect of event flapping. If the event clears and becomes set again before the hold-set timer expires, the timer is reset to the hold-set value, extending the time before another clear can take effect.

The hold-set timer must expire and the historical success rate must be met prior to the event operational state becoming cleared.

The **no** form of the command deletes the specific IP host monitoring event. The event can be deleted at any time. When the event is deleted, the in-use priority of all associated virtual router instances must be re-evaluated. The event hold-set timer has no effect on the removal procedure.

Default no host-unreachable

Parameters *ip-address* — specifies the IP address of the host for which the specific event monitors connectivity. The IP address can only be monitored by a single event in this policy. The IP address can be monitored by multiple VRRP priority control policies. The IP address can be used in one or more ping requests. Each VRRP priority control host unreachable and ping destined for the same IP address is uniquely identified on a per-message basis. Each session originates a unique identifier value for the ICMP echo request messages it generates. This allows received ICMP echo reply messages to be directed to the appropriate sending application.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x[-interface]
	x: [0 to FFFF]H
	interface: 32 chars maximum, mandatory for link-local addresses

Note: The link-local IPv6 address must have an interface name specified. The global IPv6 address must not have an interface name specified.

lag-port-down

Syntax [**no**] **lag-port-down** *lag-id*

Context config>vrrp>policy>priority-event

Description This command enables the context to configure Link Aggregation Group (LAG) priority control events that monitor the operational state of the links in the LAG.

The **lag-port-down** command configures a priority control event. The event monitors the operational state of each port in the specified LAG. When one or more of the ports enter the operationally down state, the event is considered to be set. When all the ports enter the operationally up state, the event is considered to be clear. As ports enter the operational up state, any previous set threshold that represents more down ports is considered cleared, while the event is considered to be set.

Multiple unique **lag-port-down** event nodes can be configured within the **priority-event** node up to the maximum of 32 events.

The **lag-port-down** command can reference any LAG. The *lag-id* must exist within the system. The operational state of the **lag-port-down** event will indicate:

- Set – non-existent
- Set – one port down
- Set – two ports down
- Set – three ports down
- Set – four ports down
- Set – five ports down

- Set – six ports down
- Set – seven ports down
- Set – eight ports down
- Cleared – all ports up

When the *lag-id* is created, or a port in the *lag-id* becomes operationally up or down, the event operational state is updated appropriately.

When one or more of the LAG composite ports enters the operationally down state or the *lag-id* is deleted or does not exist, the event is considered to be set. When an event transitions from clear to set, the set is processed immediately and is reflected in the associated virtual router instance's in-use priority value. As the event transitions from clear to set, a hold-set timer is loaded with the value configured by the events **hold-set** command. This timer prevents the event from clearing until it expires, damping the effect of event flapping. If the event clears and becomes set again before the hold-set timer expires, the timer is reset to the **hold-set** value, extending the time before another clear can take effect.

The **lag-port-down** event is considered to have a tiered event set state. While the priority impact per number of ports down is configurable, as more ports go down, the effect on the associated virtual router instance's in-use priority value is expected to increase (lowering the priority). When each configured threshold is crossed, any higher thresholds are considered further event sets and are processed immediately with the hold-set timer reset to the configured value of the **hold-set** command. As the thresholds are crossed in the opposite direction (fewer ports down than previously), the priority effect of the event is not processed until the hold-set timer expires. If the **number-down** threshold again increases before the hold-set timer expires, the timer is only reset to the **hold-set** value if the number of ports down is equal to or greater than the threshold that set the timer.

The event contains **number-down** nodes that define the priority delta or explicit value to be used based on the number of LAG composite ports that are in the operationally down state. These nodes represent the event set thresholds. Not all port down thresholds must be configured. As the number of down ports increases, the **number-down** *ports-down* node that expresses a value equal to or less than the number of down ports determines the delta or explicit priority value to be applied.

The **no** form of the command deletes the specific LAG monitoring event. The event can be removed at any time. When the event is removed, the in-use priority of all associated virtual router instances must be re-evaluated. The event's **hold-set** timer has no effect on the removal procedure.

Default no lag-port-down (no LAG priority control events are created)

Parameters *lag-id* — specifies the LAG ID that the specific event is to monitor, expressed as a decimal integer. The *lag-id* can only be monitored by a single event in this policy. The LAG may be monitored by multiple VRRP priority control policies. A port within the LAG and the LAG ID itself are considered to be separate entities. A composite port may be monitored with the **port-down** event while the *lag-id* the port is in is monitored by a **lag-port-down** event in the same policy.

Values 1 to 32

port-down

Syntax **port-down** *port-id*
no port-down

Context config>vrrp>policy>priority-event

Description This command configures a port down priority control event that monitors the operational state of a port. When the port enters the operationally down state, the event is considered set. When the port enters the operationally up state, the event is considered cleared.

Up to 32 unique port-down events can be defined in any combination of types.

The **port-down** command can be use on ports even if the ports are not preprovisioned or populated. The operational state of the port-down event can be one of the following states:

- set – non-provisioned
- set – not-populated
- set – down
- cleared – up

When the port is provisioned, populated, or enters the operationally up or down state, the event operational state is updated appropriately.

When the event enters the operationally down, non-provisioned, or non-populated state, the event is considered to be set. When an event transitions from clear to set, the set is processed immediately and must be reflected in the associated virtual router instance in-use priority value. As the event transitions from cleared to set, the hold-set timer is started. This timer prevents the event from clearing until it expires, damping the effect of event flapping. If the event clears and becomes set again before the hold-set timer expires, the timer is reset to the hold-set value, extending the time before another clear can take effect.

When the event enters the operationally up state, the event is considered to be cleared. Once the event hold-set expires, the effects of the event priority value are immediately removed from the in-use priority of all associated virtual router instances.

The actual effect on the virtual router instance in-use priority value depends on the defined event priority and its delta or explicit nature.

The **no** form of the command deletes the specific port monitoring event. The event can be removed at any time. If the event is removed, the in-use priority of all associated virtual router instances is re-evaluated. The event's hold-set timer has no effect on the removal procedure.

Default no port-down

Parameters *port-id* — specifies the port ID of the port monitored by the VRRP priority control event.
VRRP is supported on Ethernet adapter cards only.

The port ID can only be monitored by a single event in this policy. The port can be monitored by multiple VRRP priority control policies.

If the port is provisioned, but the port has not been populated, the appropriate event operational state is set – not populated.

If the port is not provisioned, the event operational state is set – non-provisioned.

Values

port-id	*slot*/*mda*/*port*	
bundle-id	**bundle**-*type*-*slot*/*mda*.*bundle-num*	
	type	**ima**, **ppp**
	bundle-num	1 to 128

route-unknown

Syntax [**no**] **route-unknown** *ip-prefix/mask*
[**no**] **route-unknown** *ipv6-address/prefix-length*

Context config>vrrp>policy>priority-event

Description This command enables the context to configure a route unknown priority control event that monitors the existence of a specific active IP route prefix within the routing table.

The **route-unknown** command configures a priority control event that defines a link between the VRRP priority control policy and the RTM. The RTM registers the specified route prefix as monitored by the policy. If any change (add, delete, new next hop) occurs relative to the prefix, the policy is notified and takes proper action according to the priority event definition. If the route prefix exists and is active in the routing table according to the conditions defined, the event is in the cleared state. If the route prefix is removed, becomes inactive, or fails to meet the event criteria, the event is in the set state.

Up to 32 route-unknown events can be configured.

The **route-unknown** command can reference any valid IP address mask-length pair. The IP address and associated mask length define a unique IP router prefix. The dynamic monitoring of the route prefix results in one of the following event operational states:

Route Unknown Operational State	Description
Set – non-existent	The route does not exist in the route table
Set – inactive	The route exists in the route table but is not being used
Set – wrong next hop	The route exists in the route table but does not meet the next-hop requirements
Set – wrong protocol	The route exists in the route table but does not meet the protocol requirements
Set – less specific found	The route exists in the route table but is not an exact match and does not meet any less-specific requirements
Set – default best match	The route exists in the route table as the default route but the default route is not allowed for route matching

Cleared – less specific found	A less-specific route exists in the route table and meets all criteria including the less-specific requirements
Cleared – found	The route exists in the route table manager and meets all criteria

An existing route prefix in the RTM must be active (used by the IP forwarding engine) to clear the event operational state. It can be less specific (the defined prefix can be contained in a larger prefix according to CIDR techniques) if the event has the less-specific statement defined. The less-specific route that incorporates the router prefix can be the default route (0.0.0.0). If the less-specific **allow-default** statement is defined. The matching prefix can be required to have a specific next-hop IP address if defined by the event **next-hop** command. Finally, the source of the RTM prefix can be required to be one of the dynamic routing protocols or be statically defined if defined by the event **protocol** command. If an RTM prefix is not found that matches all the above criteria (if defined in the event control commands), the event is considered to be set. If a matching prefix is found in the RTM, the event is considered to be cleared.

If an event transitions from clear to set, the set is processed immediately and must be reflected in the associated virtual router instance in-use priority value. As the event transitions from clear to set, the hold-set timer is started. This timer prevents the event from clearing until it expires, damping the effect of event flapping. If the event clears and becomes set again before the hold-set timer expires, the timer is reset to the hold-set value, extending the time before another clear can take effect.

The **no** form of the command is used to remove the specific IP prefix mask monitoring event. The event can be removed at any time. When the event is removed, the in-use priority of all associated virtual router instances must be re-evaluated. The event hold-set timer has no effect on the removal procedure.

Default no route-unknown

Parameters *ip-prefix* — specifies the IPv4 prefix address to be monitored by the route-unknown priority control event

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

mask — specifies the subnet mask length associated with the IPv4 prefix defining the route prefix to be monitored by the route-unknown priority control event

Values 0 to 32

ipv6-address — specifies the IPv6 address to be monitored by the route-unknown priority control event

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x [0 to FFFF]H

prefix-length — specifies the prefix length associated with the IPv6 address defining the route prefix to be monitored by the route-unknown priority control event

Values 1 to 128

drop-count

Syntax **drop-count** *count*
no drop-count

Context config>vrrp>policy>priority-event>host-unreachable

Description This command configures the number of consecutively sent ICMP echo request messages that must fail before the host unreachable priority control event is set.

The **drop-count** command is used to define the number of consecutive message send attempts that must fail for the host unreachable priority event to enter the set state. Each unsuccessful attempt increments the event consecutive message drop counter. With each successful attempt, the event consecutive message drop counter resets to 0.

If the event consecutive message drop counter reaches the drop-count value, the host unreachable priority event enters the set state.

The event hold-set value defines how long the event must stay in the set state even when a successful message attempt clears the consecutive drop counter. The event is not cleared until the consecutive drop counter is less than the drop-count value and the hold-set timer has a value of 0 (expired).

The **no** form of the command reverts to the default value of 3. Three consecutive ICMP echo request failures are required before the host unreachable priority control event is set.

Default 3

Parameters *count* — specifies the number of ICMP echo request message attempts that must fail for the event to enter the set state. The *count* parameter defines the threshold so that a lower consecutive number of failures can clear the event state.

Values 1 to 60

hold-clear

Syntax **hold-clear** *seconds*
no hold-clear

Context config>vrrp>policy>priority-event>host-unreachable
config>vrrp>policy>priority-event>lag-port-down
config>vrrp>policy>priority-event>port-down
config>vrrp>policy>priority-event>route-unknown

Description This command configures the hold-clear time for the event. The hold-clear time is used to prevent blackhole conditions if a virtual router instance advertises itself as a master before other conditions associated with the cleared event have had a chance to enter a forwarding state.

Default no hold-clear

Parameters *seconds* — specifies the amount of time in seconds by which the effect of a cleared event on the associated virtual router instance is delayed

Values 0 to 86400

hold-set

Syntax **hold-set** *seconds*
no hold-set

Context config>vrrp>policy>priority-event>host-unreachable
config>vrrp>policy>priority-event>lag-port-down
config>vrrp>policy>priority-event>port-down
config>vrrp>policy>priority-event>route-unknown

Description This command specifies the amount of time that must pass before the set state for a VRRP priority control event can transition to the cleared state to dampen flapping events. A flapping event continually transitions between clear and set.

The **hold-set** command dampens the effect of a flapping event. The hold-set timer prevents a set event from transitioning to the cleared state until it expires.

Each time an event transitions between cleared and set, the timer begins a countdown to 0. When the timer reaches 0, the event is allowed to enter the cleared state. Entering the cleared state is dependent on the object controlling the event, conforming to the requirements defined in the event itself. It is possible, on some event types, to have another set action reset the hold-set timer. This extends the amount of time that must expire before entering the cleared state.

When the hold-set timer expires and the event meets the cleared state requirements or is set to a lower threshold, the effect of the current set action on the in-use priority of the virtual router instance is removed. For lag-port-down events, this may be a decrease in the set effect if clearing the state lowers the set threshold.

The **hold-set** command can be executed at any time. If the currently configured hold-set timer value is larger than the new *seconds* setting, the timer is loaded with the new hold-set value.

The **no** form of the command reverts to the default value of 0 and the hold-set timer is disabled so that event transitions are processed immediately.

Default 0

Parameters *seconds* — specifies the number of seconds that the hold-set timer waits after an event enters a set state or enters a higher threshold set state, depending on the event type.

The value of 0 disables the hold-set timer, preventing any delay in processing lower set thresholds or cleared events.

Values 0 to 86400

interval

Syntax **interval** *seconds*
no interval

Context config>vrrp>policy>priority-event>host-unreachable

Description This command configures the number of seconds between host-unreachable priority event ICMP echo request messages directed to the host IP address.

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

Default 1

Parameters *seconds* — specifies the amount of time between the ICMP echo request messages sent to the host IP address for the host-unreachable priority event

Values 1 to 60

less-specific

Syntax **less-specific** [**allow-default**]
no less-specific

Context config>vrrp>policy>priority-event>route-unknown

Description This command allows a CIDR shortest-match hit on a route prefix that contains the IP route prefix associated with the route-unknown priority event.

The **less-specific** command modifies the search parameters for the IP route prefix specified in the route-unknown priority event.

The **less-specific** command makes the RTM lookup criteria less restrictive when searching for the IP prefix mask. When the route-unknown priority event sends the prefix to the RTM (as if it was a destination lookup), the matching prefix (if a result is found) is checked to see if it is an exact match or a less-specific match. The **less-specific** command enables a less-specific route table prefix to match the configured prefix. If less-specific is not specified, a less-specific route table prefix fails to match the configured prefix. The **allow-default** optional keyword extends the less-specific match to include the default route (0.0.0.0).

The **no** form of the command prevents RTM lookup results that are less specific than the route prefix from matching.

The default value specifies that the route-unknown priority event requires an exact IP prefix mask match.

Default no less-specific

Parameters **allow-default** — specifies that an RTM return of 0.0.0.0 matches the IP prefix. If the **less-specific** command is entered without the **allow-default** keyword, a return of 0.0.0.0 will not match the IP prefix.

next-hop

Syntax [**no**] **next-hop** *ip-address*

Context config>vrrp>policy>priority-event>route-unknown

Description This command adds an allowed next-hop IP address to match the IP route prefix for a route-unknown priority control event.

If the next-hop IP address does not match one of the defined IP addresses, the match is considered unsuccessful and the route-unknown event transitions to the set state.

The **next-hop** command is optional. If no next-hop IP address commands are configured, the comparison between the RTM prefix return and the route-unknown IP route prefix are not included in the next-hop information.

If more than one next-hop IP address is eligible for matching, a **next-hop** command must be executed for each IP address. Defining the same IP address multiple times has no effect after the first instance.

The **no** form of the command removes the IP address from the list of acceptable next hops when looking up the route-unknown prefix. If this IP address is the last next hop defined on the route-unknown event, the returned next-hop information is ignored when testing the match criteria. If the IP address does not exist, the **no next-hop** command returns a warning message, but continues to execute if part of the exec script.

The default value specifies that no next-hop IP address for the route-unknown priority control event is defined.

Default no next-hop

Parameters *ip-address* — specifies an acceptable next-hop IP address for a returned route prefix from the RTM when looking up the route-unknown route prefix

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x[-interface]
	x: [0 to FFFF]H
	interface: 32 chars maximum, mandatory
	for link-local addresses

Note: The link-local IPv6 address must have an interface name specified. The global IPv6 address must not have an interface name specified.

number-down

Syntax [**no**] **number-down** *number-of-lag-ports-down*

Context config>vrrp>policy>priority-event>lag-port-down

Description This command enables the context to configure an event set threshold within a lag-port-down priority control event.

The **number-down** command defines a sub-node within the **lag-port-down** event and is uniquely identified with the *number-of-lag-ports-down* parameter. Each **number-down** node within the same **lag-port-down** event node must have a unique *number-of-lag-ports-down* value. Each **number-down** node has its own **priority** command that takes effect whenever that node represents the current threshold.

The total number of sub-nodes (uniquely identified by the *number-of-lag-ports-down* parameter) allowed in a single **lag-port-down** event is equal to the total number of possible physical ports allowed in a LAG.

A **number-down** node is not required for each possible number of ports that could be down. The active threshold is always the closest lower threshold. When the number of ports down equals a given threshold, that threshold is the active threshold.

The **no** form of the command deletes the event set threshold. The threshold may be removed at any time. If the removed threshold is the current active threshold, the event set thresholds must be re-evaluated after removal.

Default no number-down (no threshold for the LAG priority event is created)

Parameters *number-of-lag-ports-down* — specifies the number of LAG ports down to create a set event threshold. This is the active threshold when the number of down ports in the LAG equals or exceeds *number-of-lag-ports-down*, but does not equal or exceed the next highest configured *number-of-lag-ports-down*.

Values 1 to 64 (applies to 64-link LAG)
1 to 32 (applies to other LAGs)

priority

Syntax **priority** *priority-level* [**delta** | **explicit**]
no priority

Context config>vrrp>policy>priority-event>host-unreachable
config>vrrp>policy>priority-event>lag-port-down>number-down
config>vrrp>policy>priority-event>port-down
config>vrrp>policy>priority-event>route-unknown

Description This command controls the effect that the set event has on the virtual router instance in-use priority.

When the event is set, the priority level is either subtracted from the base priority of each virtual router instance or it defines the explicit in-use priority value of the virtual router instance depending on whether the **delta** or **explicit** keyword is specified.

Multiple set events in the same policy have interaction constraints:

- if any set events have an explicit priority value, all the delta priority values are ignored
- the set event with the lowest explicit priority value defines the in-use priority used by all virtual router instances associated with the policy
- if no set events have an explicit priority value, all the set events delta priority values are added and subtracted from the base priority value defined on each virtual router instance associated with the policy
- if the sum of the delta priorities exceeds the **delta-in-use-limit**, then the **delta-in-use-limit** value is used as the value subtracted from the base priority value defined on each virtual router instance associated with the policy

If the **priority** command is not configured on the priority event, the priority value defaults to 0 and the qualifier keyword defaults to delta with no impact on the in-use priority.

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

Default 0

Parameters *priority-level* — specifies the priority level adjustment value

Values 0 to 254

delta | explicit — configures what effect the priority level has on the base priority value

When **delta** is specified, the priority level value is subtracted from the base priority of the associated virtual router instance when the event is set and no explicit events are set. The sum of the priority event priority level values on all set delta priority events are subtracted from the virtual router base priority to derive the virtual router instance in-use priority value. If the delta priority event is cleared, the priority level is no longer used in the in-use priority calculation.

When **explicit** is specified, the priority level value is used to override the base priority of the virtual router instance if the priority event is set and no other explicit priority event is set with a lower priority level. The set explicit priority value with the lowest priority level determines the actual in-use protocol value for all virtual router instances associated with the policy.

Default delta

protocol

Syntax **protocol** *protocol*
no protocol

Context config>vrrp>policy>priority-event>route-unknown

Description This command adds one or more route sources to match the route-unknown IP route prefix for a route-unknown priority control event.

If the route source does not match one of the defined protocols, the match is considered unsuccessful and the route-unknown event transitions to the set state.

The **protocol** command is optional. If the **protocol** command is not executed, the comparison between the RTM prefix return and the route-unknown IP route prefix does not include the source of the prefix. The **protocol** command cannot be executed without at least one associated route source keyword. All keywords are reset each time the command is executed, and only the explicitly defined protocols are allowed to match.

The **no** form of the command removes protocol route source as a match criteria for returned RTM route prefixes.

To remove specific existing route source match criteria, execute the **protocol** command and include only the specific route source criteria. Any unspecified route source criteria is removed.

Default no protocol

Parameters *protocol* — specifies the routing protocol to be used as a match criteria

Values bgp, bgp-vpn, ospf, isis, rip, static

bgp — defines BGP as an eligible route source for a returned route prefix from the RTM when looking up the route-unknown route prefix. The **bgp** keyword is not exclusive from the other available protocol keywords. If the **protocol** command is executed without the **bgp** keyword, a returned route prefix with a source of BGP is not considered a match and causes the event to enter the set state.

bgp-vpn — defines BGP-VPN as an eligible route source for a returned route prefix from the RTM when looking up the route-unknown route prefix. The **bgp-vpn** keyword is not exclusive from the other available protocol keywords. If the **protocol** command is executed without the **bgp-vpn** keyword, a returned route prefix with a source of BGP-VPN is not considered a match and causes the event to enter the set state.

isis	defines IS-IS as an eligible route source for a returned route prefix from the RTM when looking up the route-unknown route prefix. The **isis** keyword is not exclusive from the other available protocol keywords. If the **protocol** command is executed without the **isis** keyword, a returned route prefix with a source of IS-IS is not considered a match and causes the event to enter the set state.
ospf	defines OSPF as an eligible route source for a returned route prefix from the RTM when looking up the route-unknown route prefix. The **ospf** keyword is not exclusive from the other available protocol keywords. If the **protocol** command is executed without the **ospf** keyword, a returned route prefix with a source of OSPF is not considered a match and causes the event to enter the set state.
rip	defines RIP as an eligible route source for a returned route prefix from the RTM when looking up the route-unknown route prefix. The **rip** keyword is not exclusive from the other available protocol keywords. If the **protocol** command is executed without the **rip** keyword, a returned route prefix with a source of RIP is not considered a match and causes the event to enter the set state.
static	defines a static route as an eligible route source for a returned route prefix from the RTM when looking up the route-unknown route prefix. The **static** keyword is not exclusive from the other available protocol keywords. If the **protocol** command is executed without the **static** keyword, a returned route prefix with a source of static route is not considered a match and causes the event to enter the set state.

timeout

Syntax **timeout** *seconds*
no timeout

Context config>vrrp>policy>priority-event>host-unreachable

Description This command defines the time, in seconds, that must pass before considering the far-end IP host unresponsive to an outstanding ICMP echo request message.

The timeout value is not directly related to the configured interval parameter. The timeout value can be larger, equal, or smaller, relative to the interval value. If the timeout value is larger than the interval value, multiple ICMP echo request messages can be outstanding. Every ICMP echo request message transmitted to the far-end host is tracked individually according to the message identifier and sequence number.

With each consecutive attempt to send an ICMP echo request message, the timeout timer is started. The timer decrements until:

- an internal error occurs preventing message sending (request unsuccessful)
- an internal error occurs preventing message reply receiving (request unsuccessful)
- a required route table entry does not exist to reach the IP address (request unsuccessful)
- a required ARP entry does not exist and ARP request timed out (request unsuccessful)
- a valid reply is received (request successful)

Note: A required ARP request can succeed or time out after the message timeout timer expires. In this case, the message request is unsuccessful.

If an ICMP echo reply message is not received prior to the timeout period for a given ICMP echo request, that request is considered to be dropped and the consecutive message drop counter is incremented for the priority event.

If an ICMP echo reply message with the same sequence number as an outstanding ICMP echo request message is received prior to that message timing out, the request is considered successful. The consecutive message drop counter is cleared and the request message no longer is outstanding.

If an ICMP echo reply message with a sequence number equal to an ICMP echo request sequence number that had previously timed out is received, that reply is silently discarded while incrementing the priority event reply discard counter.

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

Default 1

Parameters *seconds* — specifies the amount of time before an ICMP echo request message is timed out. Once a message is timed out, a reply with the same identifier and sequence number is discarded.

Values 1 to 60

4.13.2.2 VRRP Show Commands

Note: The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

policy

Syntax **policy** [*policy-id* [**event** *event-type specific-qualifier*]]

Context show>vrrp

Description This command displays VRRP priority control policy information.

Parameters *policy-id* — displays statistics for the specified priority control policy ID

Values 1 to 9999

Default all VRRP policy IDs

event-type — displays information on the specified VRRP priority control event within the policy ID

Values **port-down** *port-id*
lag-port-down *lag-id*
host-unreachable *host-ip-addr*
route-unknown *route-prefix/mask*

Default all event types and qualifiers

specific-qualifier — displays information about the specific qualifier

Values *port-id*, *lag-id*, *host-ip-addr*, *route-prefix/mask*

Output The following outputs are examples of VRRP policy summary information:

- Policy summary (Output Example (summary))
- Policy event port-down summary (Output Example (port-down))
- Policy event lag-port-down summary (Output Example (lag-port-down))
- Policy event host-unreachable summary (Output Example (host-unreachable))
- Policy event route-unknown summary (Output Example (route-unknown))
- Summary of policy output fields (Table 68)

Output Example (summary)

```
show vrrp policy 1
*A:7705:Dut-A # show vrrp policy 1
===============================================================================
VRRP Policy 1
===============================================================================
Description    :
Current Priority: 120 Delta           Applied           : Yes
Current Explicit: None                Current Delta Sum : 120
Delta Limit     : 1                   Svc Context       : None

-------------------------------------------------------------------------------
Rtr Id/    Applied To                      VR   Opr  Base In-use Master Is
Svc Id     Interface Name                  Id        Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
           vrrpMasNode                     10   Up   250  130    200    No

-------------------------------------------------------------------------------
Rtr Id/    Applied To                      IPv6 Opr  Base In-use Master Is
Svc Id     Interface Name                  VR-Id     Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
SRRP       Applied To Interface Name       Oper      Base     In-use    Master
Id         Rtr Id/Svc                      State     Pri      Pri       Pri
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
Priority Control Events
-------------------------------------------------------------------------------
Event Type & ID                Event Oper State        Hold Set  Priority In
                                                       Remaining &Effect  Use
-------------------------------------------------------------------------------
Route Unknown 10.20.20.3/32    Set-NonExistant         Expired   120 Del  Yes
LAG Port Down 1                n/a                     Expired       --   No
    2 Number Down                                                 12 Del
===============================================================================
```

Output Example (port-down)

```
show vrrp policy 1 event port-down
*A:7705:Dut-A# show vrrp policy 1 event port-down 1/1/8
===============================================================================
VRRP Policy 1, Event Port Down 1/1/8
===============================================================================
Description     :
Current Priority: None                Applied           : Yes
Current Explicit: None                Current Delta Sum : None
Delta Limit     : 1                   Svc Context       : None

-------------------------------------------------------------------------------
Rtr Id/    Applied To                      VR   Opr  Base In-use Master Is
Svc Id     Interface Name                  Id        Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
           vrrpMasNode                     10   Up   250  250    250    Yes
```

```
-------------------------------------------------------------------------------
Rtr Id/    Applied To                       IPv6 Opr  Base In-use Master Is
Svc Id     Interface Name                   VR-Id     Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
SRRP       Applied To Interface Name        Oper      Base     In-use    Master
Id         Rtr Id/Svc                       State     Pri      Pri       Pri
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
Priority Control Event Port Down 1/1/8
-------------------------------------------------------------------------------
Priority        : 120                  Priority Effect   : Delta
Hold Set Config : 10 sec               Hold Set Remaining: Expired
Hold Clr Config : 0 sec                Hold Clr Remaining: Expired
Value In Use    : No                   Current State     : Cleared
# trans to Set  : 0                    Previous State    : Cleared
Last Transition : 01/21/2013 16:38:27
===============================================================================
```

Output Example (lag-port-down)

```
*A:Sar18 Dut-A# show vrrp policy 12 event lag-port-down 1
===============================================================================
VRRP Policy 12, Event LAG Port Down 1
===============================================================================
Description     : test_policy_12
Current Priority: None                 Applied           : No
Current Explicit: None                 Current Delta Sum : None
Delta Limit     : 1                    Svc Context       : None
-------------------------------------------------------------------------------
Rtr Id/    Applied To                       VR   Opr  Base In-use Master Is
Svc Id     Interface Name                   Id        Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
None
-------------------------------------------------------------------------------
Rtr Id/    Applied To                       IPv6 Opr  Base In-use Master Is
Svc Id     Interface Name                   VR-Id     Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
None
-------------------------------------------------------------------------------
SRRP        Applied To Interface Name        Oper          Base  In-use Master
Id          Rtr Id/Svc Id                    State         Pri   Pri    Pri
-------------------------------------------------------------------------------
None
-------------------------------------------------------------------------------
Priority Control Event LAG Port Down 1
-------------------------------------------------------------------------------
Hold Set Config : 0 sec                Hold Set Remaining: Expired
Hold Clr Config : 0 sec                Hold Clr Remaining: Expired
Value In Use    : No                   Current State     : n/a
# trans to Set  : 0                    Previous State    : n/a
Last Transition : 04/25/2017 19:33:37
-------------------------------------------------------------------------------
```

```
Number Down Threshold    Event Priority      Event Type
-------------------------------------------------------------------------------
2                        12                  Delta
===============================================================================
```

Output Example (host-unreachable)

```
show vrrp policy 1 event host-unreachable
*A:7705:Dut-A# show vrrp policy 1 event host-unreachable 10.20.20.3
===============================================================================
VRRP Policy 1, Event Host Unreachable 10.20.20.3
===============================================================================
Description     :
Current Priority: None                Applied           : Yes
Current Explicit: None                Current Delta Sum : None
Delta Limit     : 1                   Svc Context       : None

-------------------------------------------------------------------------------
Rtr Id/    Applied To                       VR   Opr  Base In-use Master Is
Svc Id     Interface Name                   Id        Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
           vrrpMasNode                      10   Up   250  250    250    Yes
-------------------------------------------------------------------------------
Rtr Id/    Applied To                       IPv6 Opr  Base In-use Master Is
Svc Id     Interface Name                   VR-Id     Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
SRRP       Applied To Interface Name        Oper      Base     In-use    Master
Id         Rtr Id/Svc                       State     Pri      Pri       Pri
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
Priority Control Event Host Unreachable 10.20.20.3
-------------------------------------------------------------------------------
Priority        : 120                 Priority Effect   : Delta
Interval        : 1 sec               Timeout           : 1 sec
Drop Count      : 3
Hold Set Config : 0 sec               Hold Set Remaining: Expired
Hold Clr Config : 0 sec               Hold Clr Remaining: Expired
Value In Use    : No                  Current State     : Cleared-ReplyReceived
# trans to Set  : 0                   Previous State    : Cleared-ReplyReceived
Last Transition : 01/21/2013 16:38:27
===============================================================================
```

Output Example (route-unknown)

```
show vrrp policy 1 event route-unknown
 *A:7705:Dut-A#show vrrp policy 1 event route-unknown 10.20.20.3/32
===============================================================================
VRRP Policy 1, Event Route Unknown 10.20.20.3/32
===============================================================================
Description     :
Current Priority: 120 Delta           Applied           : Yes
Current Explicit: None                Current Delta Sum : 120
Delta Limit     : 1                   Svc Context       : None

-------------------------------------------------------------------------------
Rtr Id/    Applied To                      VR   Opr  Base In-use Master Is
Svc Id     Interface Name                  Id        Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
           vrrpMasNode                     10   Up   250  130    200    No
-------------------------------------------------------------------------------
Rtr Id/    Applied To                      IPv6 Opr  Base In-use Master Is
Svc Id     Interface Name                  VR-Id     Pri  Pri    Pri    Master
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
SRRP       Applied To Interface Name       Oper      Base     In-use    Master
Id         Rtr Id/Svc                      State     Pri      Pri       Pri
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
Priority Control Event Route Unknown 10.20.20.3/32
-------------------------------------------------------------------------------
Priority        : 120                 Priority Effect   : Delta
Less Specific   : No                  Default Allowed   : No
Next Hop(s)     : None
Protocol(s)     : None
Hold Set Config : 0 sec               Hold Set Remaining: Expired
Hold Clr Config : 0 sec               Hold Clr Remaining: Expired
Value In Use    : Yes                 Current State     : Set-NonExistant
# trans to Set  : 1                   Previous State    : Cleared-Found
Last Transition : 01/21/2013 17:14:55
===============================================================================
```

Table 68 VRRP Policy and Policy Event Summary Field Descriptions

Label	Description
Current Priority	The base router priority for the virtual router instance used in the master election process
Applied	The number of virtual router instances to which the policy has been applied. The policy cannot be deleted unless this value is 0

Table 68 **VRRP Policy and Policy Event Summary Field Descriptions (Continued)**

Label	Description
Current Explicit	When multiple explicitly defined events associated with the priority control policy happen simultaneously, the lowest value of all the current explicit priorities will be used as the in-use priority for the virtual router
Current Delta Sum	The sum of the priorities of all the delta events when multiple delta events associated with the priority control policy happen simultaneously. This sum is subtracted from the base priority of the virtual router to give the in-use priority.
Delta Limit	The delta-in-use-limit for a VRRP policy. Once the total sum of all delta events has been calculated and subtracted from the base-priority of the virtual router, the result is compared to the delta-in-use-limit value. If the result is less than this value, the delta-in-use-limit value is used as the virtual router in-use priority value. If an explicit priority control event overrides the delta priority control events, the delta-in-use-limit has no effect.
Svc Context	The service context
Rtr Id/Svc Id	The router ID or service ID to which the VRRP policy is applied
Applied To Interface Name	The interface name where the VRRP policy is applied
VR Id	The virtual router ID for the IPv4 interface
IPv6 VR Id	The virtual router ID for the IPv6 interface
Opr	The operational state of the virtual router
Base Pri	The base priority used by the virtual router instance
In-use Pri	The current in-use priority associated with the VRRP virtual router instance
Master Pri	The priority of the virtual router instance that is the current master
Is Master	Indicates whether the router is configured as the virtual router master
SRRP ID	The subscriber routed redundancy protocol (SRRP) ID Not applicable to the 7705 SAR
Oper State	The operational state of the SRRP
Event Type & ID	The event-type and ID for types such as port-down, lag-port-down, host-unreachable, or route-unknown

Table 68 **VRRP Policy and Policy Event Summary Field Descriptions (Continued)**

Label	Description
Priority & Effect	Delta — a conditional event defined in a priority control policy that subtracts a given amount from the base priority to give the current in-use priority for the VRRP virtual router instances to which the policy is applied Explicit— a conditional event defined in a priority control policy that explicitly defines the in-use priority for the VRRP virtual router instances to which the policy is applied. Explicit events override all delta events. When multiple explicit events occur simultaneously, the event with the lowest priority value defines the in-use priority.
Event Opr State	The operational state of the priority event
In Use	Indicates whether the priority event is in use
Hold Set Config	The configured number of seconds that the hold-set timer waits after an event enters a set state or enters a higher threshold set state, depending on the event type
Hold Set Remaining	The remaining amount of time that must pass before the set state for a VRRP priority control event can transition to the cleared state to dampen flapping events
Hold Clr Config	The configured amount of time that must pass before the clear state for a VRRP priority control event can transition to the set state to dampen flapping events
Hold Clr Remaining	The remaining amount of time that must pass before the clear state for a VRRP priority control event can transition to the set state to dampen flapping events
Value In Use	Yes — the event is currently affecting the in-use priority of some virtual router No — the event is not affecting the in-use priority of some virtual router
Current State	The current state of the priority event
# trans to Set	The number of times the event has transitioned to one of the set states
Previous State	The previous state of the priority event
Last Transition	The date and time of the last state transition for the priority event
Number Down Threshold	The number of LAG ports down to create a set event threshold

Table 68 **VRRP Policy and Policy Event Summary Field Descriptions (Continued)**

Label	Description
Event Priority	The priority value that is either subtracted from the base priority of each virtual router instance (delta) or defined as the explicit in-use priority value of the virtual router instance
Event Type	The event type: Delta or Explicit
Priority	The priority value configured on the event
Priority Effect	The effect that the set event has on the virtual router instance in-use priority When the event is set, the priority level is either subtracted from the base priority of each virtual router instance or it defines the explicit in-use priority value of the virtual router instance depending on whether the **delta** or **explicit** keyword is specified
Interval	The number of seconds between host-unreachable priority event ICMP echo request messages directed to the host IP address
Timeout	The time, in seconds, that must pass before considering the far-end IP host-unresponsive to an outstanding ICMP echo request message
Drop Count	The number of consecutively sent ICMP echo request messages that must fail before the host unreachable priority control event is set
Less Specific	Modifies the search parameters for the IP route prefix specified in the route-unknown priority event. Using this command allows a CIDR shortest-match hit on a route prefix that contains the IP route prefix
Default Allowed	Indicates whether the less-specific match includes the default route (0.0.0.0)
Next Hop(s)	The next-hop IP address to match the IP route prefix for a route-unknown priority control event.
Protocol(s)	The protocol included with other match criteria to determine the transition state

vrrp

Syntax **vrrp**

Context show>router>vrrp

Description This command displays information for the VRRP instance.

instance

Syntax **instance** [**interface** *interface-name* [**vrid** *virtual-router-id*]
instance [**interface** *interface-name* **vrid** *virtual-router-id* **ipv6**

Context show>router>vrrp

Description This command displays information for the VRRP instance.

Parameters *interface-name* — displays status and statistics for the specified interface

virtual-router-id — displays statistics for the specified virtual router ID

Values 1 to 255

ipv6 — specifies the IPv6 instance

Output The following output is an example of a router VRRP instance summary information, and Table 69 describes the fields.

Output Example

```
show router vrrp instance interface n2 vrid 1
 *A:7705:Dut-A# show router 10 vrrp instance interface vrrpMasNode vrid 10
===============================================================================
VRRP Instance 10 for interface "vrrpMasNode"
===============================================================================
Owner               : Yes                 VRRP State        : Master
Primary IP of Master: 192.168.0.1 (Self)
Primary IP          : 192.168.0.1         Standby-Forwarding: Disabled
VRRP Backup Addr    : 192.168.0.1
Admin State         : Up                  Oper State        : Up
Up Time             : 01/21/2013 18:29:17 Virt MAC Addr     : 00:00:5e:00:01:0a
Auth Type           : None
Config Mesg Intvl   : 1                   In-Use Mesg Intvl : 1
Base Priority       : 255                 In-Use Priority   : 255
Init Delay          : 0                   Init Timer Expires: 0.000 sec
Creation State      : Active

-------------------------------------------------------------------------------
Master Information
-------------------------------------------------------------------------------
Primary IP of Master: 192.168.0.1 (Self)
Addr List Mismatch  : No                  Master Priority   : 255
Master Since        : 01/21/2013 18:29:17
```

```
-------------------------------------------------------------------------------
Masters Seen (Last 32)
-------------------------------------------------------------------------------
Primary IP of Master   Last Seen             Addr List Mismatch     Msg Count
-------------------------------------------------------------------------------
192.168.0.1            01/21/2013 18:29:17   No                            0
192.168.0.3            01/21/2013 18:28:41   No                            1

-------------------------------------------------------------------------------
Statistics
-------------------------------------------------------------------------------
Become Master       : 3                  Master Changes    : 3
Adv Sent            : 139                Adv Received      : 1
Pri Zero Pkts Sent  : 2                  Pri Zero Pkts Rcvd: 0
Preempt Events      : 0                  Preempted Events  : 0
Mesg Intvl Discards : 0                  Mesg Intvl Errors : 0
Addr List Discards  : 0                  Addr List Errors  : 0
Auth Type Mismatch  : 0                  Auth Failures     : 0
Invalid Auth Type   : 0                  Invalid Pkt Type  : 0
IP TTL Errors       : 0                  Pkt Length Errors : 0
Total Discards      : 0
```

Table 69 **Router VRRP Instance Summary Field Descriptions**

Label	Description
Owner	Yes — Specifies that the virtual router instance as owning the virtual router IP addresses
	No — Indicates that the virtual router instance is operating as a non-owner
VRRP State	Specifies whether the VRRP instance is operating in a master or backup state
Primary IP of Master	The IP address of the VRRP master
Primary IP	The IP address of the VRRP owner
Standby-Forwarding	Specifies whether this VRRP instance allows forwarding packets to a standby router
Virt MAC Addr	The virtual MAC address used in ARP responses when the VRRP virtual router instance is operating as a master
Config Mesg Intvl	The administrative advertisement message timer used by the master to send VRRP messages and to derive the master down timer as backup
Base Priority	The base-priority value used to derive the in-use priority of the virtual router instance as modified by any optional VRRP priority control policy
In-Use Priority	The current in-use priority associated with the VRRP virtual router instance

Table 69 **Router VRRP Instance Summary Field Descriptions (Continued)**

Label	Description
Master Since	The date and time when operational state of the virtual router changed to master. For a backup outer, this value specifies the date and time when it received the first VRRP message from the virtual router which is the current master.

statistics

Syntax **statistics**

Context show>router>vrrp

Description This command displays statistics for the VRRP instance.

Output The following output is an example of VRRP statistics information.

Output Example

```
*A:7705custDoc:Sar18>show>router>vrrp# statistics
===============================================================================
VRRP Global Statistics
===============================================================================
VR Id Errors       : 0                  Version Errors     : 0
Checksum Errors    : 0
===============================================================================
*A:7705custDoc:Sar18>show>router>vrrp#
```

4.13.2.3 VRRP Monitor Commands

instance

Syntax **instance interface** *interface-name* **vr-id** *virtual-router-id* [**ipv6**] [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor>router>vrrp

Description This command enables monitoring for VRRP instances.

Parameters *interface-name* — specifies the name of the existing IES or VPRN interface on which VRRP is configured

virtual-router-id — specifies the virtual router ID for the existing IES or VPRN interface, expressed as a decimal integer

Values 1 to 255

ipv6 — specifies monitoring the IPv6 instance

seconds — specifies the interval for each display in seconds

Values 3 to 60

Default 10

repeat — specifies the number of times the command is repeated

Values 1 to 999

Default 10

absolute — specifies that raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — specifies the rate per second for each statistic instead of the delta

Default delta

Output The following output is an example of a router VRRP instance summary information.

Output Example

```
monitor router vrrp instance interface n2 vrid 1

*A:7705:DutA#  monitor router vrrp instance interface vrrpMasNode vr-id 10 absolute
===============================================================================
Monitor statistics for VRRP Instance 10 on interface "vrrpMasNode"
===============================================================================
-------------------------------------------------------------------------------
At time t = 0 sec (Base Statistics)
-------------------------------------------------------------------------------
Become Master       : 0                  Master Changes    : 0
Adv Sent            : 2                  Adv Received      : 0
Pri Zero Pkts Sent  : 0                  Pri Zero Pkts Rcvd: 0
```

```
Preempt Events      : 0                   Preempted Events  : 0
Mesg Intvl Discards : 0                   Mesg Intvl Errors : 0
Addr List Discards  : 0                   Addr List Errors  : 0
Auth Type Mismatch  : 0                   Auth Failures     : 0
Invalid Auth Type   : 0                   Invalid Pkt Type  : 0
IP TTL Errors       : 0                   Pkt Length Errors : 0
Total Discards      : 0
-------------------------------------------------------------------------------
At time t = 10 sec (Mode: Absolute)
-------------------------------------------------------------------------------
Become Master       : 0                   Master Changes    : 0
Adv Sent            : 12                  Adv Received      : 0
Pri Zero Pkts Sent  : 0                   Pri Zero Pkts Rcvd: 0
Preempt Events      : 0                   Preempted Events  : 0
Mesg Intvl Discards : 0                   Mesg Intvl Errors : 0
Addr List Discards  : 0                   Addr List Errors  : 0
Auth Type Mismatch  : 0                   Auth Failures     : 0
Invalid Auth Type   : 0                   Invalid Pkt Type  : 0
IP TTL Errors       : 0                   Pkt Length Errors : 0
Total Discards      : 0
-------------------------------------------------------------------------------
At time t = 20 sec (Mode: Absolute)
-------------------------------------------------------------------------------
Become Master       : 0                   Master Changes    : 0
Adv Sent            : 22                  Adv Received      : 0
Pri Zero Pkts Sent  : 0                   Pri Zero Pkts Rcvd: 0
Preempt Events      : 0                   Preempted Events  : 0
Mesg Intvl Discards : 0                   Mesg Intvl Errors : 0
Addr List Discards  : 0                   Addr List Errors  : 0
Auth Type Mismatch  : 0                   Auth Failures     : 0
Invalid Auth Type   : 0                   Invalid Pkt Type  : 0
IP TTL Errors       : 0                   Pkt Length Errors : 0
Total Discards      : 0
```

4.13.2.4 VRRP Clear Commands

interface

Syntax [**interface** *interface-name* [**vrid** *virtual-router-id*]
[**interface** *interface-name* **vrid** *virtual-router-id* **ipv6**

Context clear>router>vrrp

Description This command resets VRRP protocol instances on an IES or VPRN interface.

Parameters *interface-name* — specifies an existing interface name up to 32 characters in length

virtual-router-id — specifies the virtual router identifier

Values 1 to 255

ipv6 — clears IPv6 information for the specified interface

statistics

Syntax **statistics**
statistics interface *interface-name* [**vrid** *virtual-router-id*]
statistics interface *interface-name* **vrid** *virtual-router-id* **ipv6**

Context clear>router>vrrp

Description This command clears statistics for VRRP instances on an IES or VPRN interface or VRRP priority control policies.

Parameters *interface-name* — clears the VRRP statistics for all VRRP instances on the specified IES or VPRN interface

virtual-router-id — specifies the virtual router identifier

Values 1 to 255

ipv6 — clears IPv6 statistics for the specified IPv6 interface

4.13.2.5 VRRP Debug Commands

events

Syntax [**no**] **events**
[**no**] **events interface** *ip-int-name* [**vrid** *virtual-router-id*]
[**no**] **events interface** *ip-int-name* **vrid** *virtual-router-id* **ipv6**

Context debug>router>vrrp

Description This command enables or disables debugging for VRRP events.

Parameters *ip-int-name* — specifies the interface name

virtual-router-id — specifies the virtual router identifier

Values 1 to 255

ipv6 — debugs the specified IPv6 IES interface

packets

Syntax [**no**] **packets**
[**no**] **packets interface** *ip-int-name* [**vrid** *virtual-router-id*]
[**no**] **packets interface** *ip-int-name* **vrid** *virtual-router-id* **ipv6**

Context debug>router>vrrp

Description This command enables or disables debugging for VRRP packets.

Parameters *interface-name* — specifies the interface name

virtual-router-id — specifies the virtual router identifier

Values 1 to 255

ipv6 — debugs the specified IPv6 IES packets

5 Filter Policies

This chapter provides information about filter policies and management.

Topics in this chapter include:

5.1 Configuring Filter Policies

Topics in this section include:

5.1.1 Overview of Filter Policies

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

The 7705 SAR supports seven types of filter policies:

- IP filters
- MAC filters
- VLAN filters
- CSM filters
- IP exception filters
- management access filters
- match-list filters

The 7705 SAR also supports policy-based routing (PBR), which is based on IP filters, and multi-field classification (MFC).

IP, MAC, and VLAN filters scan all traffic and take the appropriate (configured) action against matching packets. Packets that are not filtered by one of these filters and are destined for the 7705 SAR are then scanned by the CSM filter, if configured.

IP exception filters scan all outbound traffic entering a Network Group Encryption (NGE) domain and allow packets that match the exception filter criteria to transit the NGE domain unencrypted.

IP and MAC filter support for SAP and SDP is described in the following sections and is summarized in Table 70 and Table 71. Ingress filter override support for routed VPLS on IES and VPRN services is summarized in Table 72. IPv4 and IPv6 filter support (ingress and egress) for network interfaces is described in the lists following Table 72. MAC filters do not support network interfaces.

Configuring an entity for a filter policy is optional. If a network or service interface is not configured with filter policies, all traffic is allowed on the interface. By default, there are no filters associated with interfaces or services. The filters must be explicitly created and associated. When you create a new filter, you must specify a unique filter ID value for each new filter policy, as well as each new filter entry and associated actions. The filter entries specify the filter matching criteria. See Filter Policy Entries. After creating a filter policy you can also, optionally, assign filters a unique name. Filter IDs or filter names can be used throughout the system to manage filter policies and assign them to interfaces.

Table 70 **IP and MAC Filter Support on SAPs**

Service SAP	Ingress Filter			Egress Filter		
	IPv4	IPv6	MAC	IPv4	IPv6	MAC
Epipe	Yes	No	No	No	No	No
IES	Yes	Yes	No	Yes	Yes	No
Ipipe	Yes	No	No	No	No	No
VPLS	Yes	Yes	Yes	Yes	Yes	Yes
VPRN	Yes	Yes	No	Yes	Yes	No

Table 71 **IP and MAC Filter Support on SDPs**

Service SDP	Ingress Filter			Egress Filter		
	IPv4	IPv6	MAC	IPv4	IPv6	MAC
Epipe	No	No	No	No	No	No
IES	Yes	No	No	No	No	No
Ipipe	No	No	No	No	No	No
VPLS	Yes	Yes	Yes	No	No	No

Table 71 **IP and MAC Filter Support on SDPs (Continued)**

Service SDP	Ingress Filter			Egress Filter		
	IPv4	IPv6	MAC	IPv4	IPv6	MAC
VPRN	Yes	Yes	No	No	No	No

Table 72 **Routed VPLS Ingress Filter Override Support**

Service	Ingress Override IPv4	Ingress Override IPv6
IES	Yes	Yes
VPRN	Yes	Yes

IP Filters

IPv4 filters can be applied to the following entities:

- network interfaces
  - ingress and egress network interfaces, affecting incoming traffic from the network link and outgoing traffic to the network link
- SAPs
  - ingress IES management SAPs, affecting incoming node management traffic
  - ingress pseudowire SAPs (Epipe and Ipipe), affecting incoming user traffic
  - ingress VPLS SAPs, affecting incoming user traffic
  - ingress VPRN SAPs and IES SAPs, affecting incoming user traffic
  - egress VPLS SAPs (Ethernet SAPs only), affecting outgoing user traffic
  - egress VPRN and IES SAPs, affecting outgoing user traffic
- SDPs
  - ingress VPLS SDPs (spoke and mesh), affecting incoming traffic from the remote end of the service
  - ingress IES and VPRN interface spoke SDPs, affecting incoming traffic from the remote end of the service

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

IPv6 filters can be applied to the following entities:

- network interfaces

  - ingress and egress Ethernet network interfaces (with null or dot1q encapsulation)
  - ingress and egress network interfaces on the 4-port OC3/STM1 Clear Channel Adapter card (with POS encapsulation)
- SAPs
  - ingress IES SAPs
  - ingress and egress VPLS SAPs
  - ingress and egress VPRN SAPs
- SDPs
  - ingress VPLS SDPs (spoke and mesh), affecting incoming traffic from the remote end of the service
  - ingress VPRN interface spoke SDPs, affecting incoming traffic from the remote end of the service

MAC Filters

MAC filters can be applied to the following entities:

- SAPs
  - ingress and egress VPLS SAPs, affecting incoming or outgoing user traffic
- SDPs
  - ingress VPLS SDPs (spoke and mesh), affecting outgoing user traffic

VLAN Filters

VLAN filters can be applied to ring ports at the ingress point on the 2-port 10GigE (Ethernet) Adapter card and 2-port 10GigE (Ethernet) module. VLAN filters are blocked on all other adapter cards and modules.

CSM Filters

The 7705 SAR supports IPv4 and IPv6 CSM filters. For information on CSM filters, refer to the 7705 SAR System Management Guide, “CSM Filters and CSM Security”.

IP Exception Filters

The 7705 SAR supports IPv4 exception filters. For information on IP exception filters, refer to the 7705 SAR Services Guide, “Router Encryption Exceptions using ACLs”.

Match List for Filter Policies

The filter **match-list ip-prefix-list** and **ipv6-prefix-list** commands define a list of IP prefixes that can be used as match criteria for adapter card IP and IPv6 filters. These commands can also be used for CPM (CSM) filters, IP exception filters, and management access filters.

A match list simplifies the filter policy configuration by allowing multiple prefixes to be listed in a single filter entry instead of creating an entry for each.

The same match list can be used in more than one filter policy. A change in match list content is automatically propagated across all policies that use that list.

Prefix-exclude

A prefix can be excluded from an IPv4 or IPv6 prefix list with the **prefix-exclude** command.

For example, when traffic needs to be rate limited to 10.0.0.0/16 with the exception of 10.0.2.0/24, the following options are available.

- By applying **prefix-exclude**, a single IP prefix list is configured with two prefixes:

```
ip-prefix-list "list-1" create
    prefix 10.0.0.0/16
    prefix-exclude 10.0.2.0/24
exit
```

- Without applying **prefix-exclude**, all eight included subnets must be manually configured in the IP prefix list:

```
ip-prefix-list "list-1" create
    prefix 10.0.0.0/23
    prefix 10.0.3.0/24
    prefix 10.0.4.0/22
    prefix 10.0.8.0/21
    prefix 10.0.16.0/20
    prefix 10.0.32.0/19
    prefix 10.0.64.0/18
    prefix 10.0.128.0/17
exit
```

Manually configuring an IP prefix list is time consuming and error-prone compared to using the **prefix-exclude** command.

The filter resources, consumed in hardware, are identical between the two configurations.

Configured **prefix-exclude** prefixes are ignored when no overlapping larger subnet is configured in the prefix list. For example: **prefix-exclude 1.1.1.1/24** is ignored if the only included subnet is 10.0.0.0/16.

5.1.2 Network and Service (Access) Interface-based Filtering

IP and MAC filter policies specify either a forward or a drop action for packets, based on information specified in the match criteria. Within each filter policy, you can create entries that define matching criteria.

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

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

Only one type of filter (IP or MAC) can be assigned to an interface at a time, and only one filter of that type can be assigned to an interface at a time. The exception is a dual-stack interface (one that supports both IPv4 and IPv6); the interface can have both an IPv4 and an IPv6 filter assigned to it.

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

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

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

5.1.3 Policy-Based Routing

Traditionally, IP routing is done by making routing decisions based on the destination IP address of the incoming packet. PBR expands the routing decision from one based solely on the destination IP address to include any other IP criteria, such as source IP address, DSCP, or source/destination UDP/TCP port.

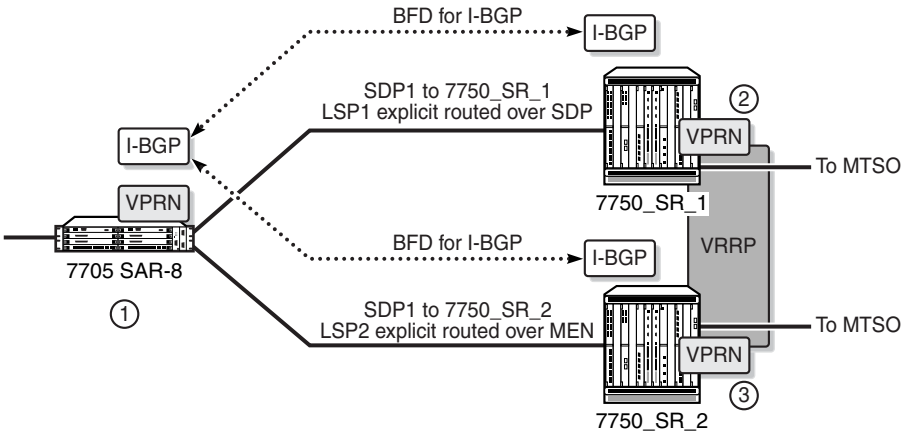
Using PBR at the iLER node provides filtering needed to route IP traffic over multiple uplink interfaces or tunnels using IP criteria. For example, a service provider can use PBR to separate high-value traffic (signaling) from user data by examining the source IP address and/or DSCP bits of the incoming IP packets, and assign a separate transport tunnel to each traffic flow. The transport tunnels could be engineered by using RSVP-TE throughout the entire mobile backhaul network with specific reservation values. The LSP is signaled throughout the network and reserves the needed resources at each node, ensuring the QoS for the high-value traffic.

PBR can also be used to extract packets from the data path and send them to the CSM for debugging or slow path forwarding.

Figure 12 illustrates a PBR implementation for VPRN services in an LTE network, and includes CLI command syntax. The 7705 SAR-8 Shelf V2 at the cell site makes routing decisions based on the incoming packet DSCP only, as follows:

- BE packets are forwarded to 7750 SR_1 over SDP1
- AF11 packets are forwarded to 7750 SR_2 over SDP2
- each SDP (SDP1 and SDP2) is signaled throughout the network using RSVP-TE protocol with its own separate TE criteria

Figure 12 **PBR Filtering Based on the DSCP of Incoming Packets**



1. 7705 SAR-8 configuration, PBR filter within VPRN commands:
   - for DSCP BE
     action forward next-hop indirect *s_rt1_ip_addr*
   - for DSCP AF11
     action forward next-hop indirect *s_rt2_ip_addr*

2. 7750_SR_1 configuration, VPRN commands:
   static-route *s_rt1_ip_addr* next-hop *to_MTSO_ip_addr* metric 50
   static-route *s_rt2_ip_addr* next-hop *to_MTSO_ip_addr* metric 1000

3. 7750_SR_2 configuration, VPRN commands:
   static-route *s_rt1_ip_addr* next-hop *to_MTSO_ip_addr* metric 1000
   static-route *s_rt2_ip_addr* next-hop *to_MTSO_ip_addr* metric 50

Note: The static routes created on the 7750 SRs are used solely for directing traffic from the 7705 SAR-8 via PBR and DSCP bits.

23687

PBR is supported at ingress for the following services and interfaces:

- IES and VPRN service
  - SAP
  - Layer 3 spoke SDP
  - routed VPLS
- router network interface (Global Routing Table (GRT))

Note: A PBR filter action can be assigned to an Epipe or Ipipe, or to VPLS (SAP, spoke SDP, or mesh SDP); however, the PBR action is ignored (not performed).

PBR is supported on the private IPSec service (VPRN). For more information on IPSec and PBR, refer to the “PBR” section in the 7705 SAR Services Guide.

5.1.4 Multi-field Classification (MFC)

Multi-field classification (MFC) allows untrusted traffic arriving on the access ports of the 7705 SAR to be reclassified and queued according to a forwarding class assigned to the traffic.

Traffic is classified based on IP criteria. Arriving traffic has an ACL (also known as filter policies) applied to it. If the ACL action is **forward fc**, a match results in the assignment of the corresponding configured Forwarding Class (FC). This FC is used for queuing of the packet through the 7705 SAR. The match can be based on any IP criteria currently supported by the 7705 SAR IP filter policies.

When MFC is configured and a match is made on an arriving packet, the FC is based only on the MFC configuration. The access ingress policy is no longer active for this packet.

Both PBR and MFC are configured under the IP filter configuration and the action of the filter policy can include both PBR (**next-hop** *ip-address*) and MFC (**fc** *fc-name*).

If MFC is assigned to a Layer 3 spoke-SDP termination interface, MFC classification is based on the traffic's customer-assigned inner IP packet. The filter policy rules are applied to the IP criteria of the inner packet after the VC label and transport tunnel label have been removed from the packet. Based on the matching criteria, the appropriate FC is assigned to the packet. This functionality allows the customer packet to be marked with the correct DSCP before it egresses the 7705 SAR. This applies only to an untrusted SAP configuration that has a SAP egress QoS policy assigned to it.

MFC is supported at ingress for the following services and interfaces:

- IES and VPRN service
  - SAP
  - Layer 3 spoke SDP
  - routed VPLS
- router network interface (Global Routing Table (GRT))
- VLLs
  - Epipe
  - Ipipe
- VPLS
  - SAP
  - spoke or mesh SDP

Multi-field classification (MFC) is also supported on the private IPSec service (VPRN). MFC functions in the same manner as the VPRN configuration of traditional services.

5.1.5 VLAN-based Filtering

VLAN filter policies specify either a forward or a drop action for packets, based on VLAN ID information specified in the policy match criteria.

Only one VLAN filter is allowed per ring port on the 2-port 10GigE (Ethernet) Adapter card or 2-port 10GigE (Ethernet) module. The same VLAN filter can be applied to both ring ports. Each VLAN filter supports up to 64 matching criteria entries. The filter acts on ingress traffic and the forwarding action sends packets to the other ring port or to the v-port, depending on the packet's destination.

The number of VLAN filters that can be created depends on the memory available on the 2-port 10GigE (Ethernet) Adapter card or 2-port 10GigE (Ethernet) module.

The 7705 SAR does not support filter logging or statistics collection for VLAN filters.

5.1.6 Filter Policy Entries

Topics in this section include:

- Applying Filter Policies
- Packet Matching Criteria
- Ordering Filter Entries

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

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

- scope (exclusive or template) (except VLAN filter policies, which always have a template scope)

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

Each filter entry contains:

- match criteria
- an action

5.1.6.1 Applying Filter Policies

IPv4 filter policies can be applied at:

- network interfaces
  - ingress and egress of network IP interfaces
- SAPs
  - ingress of Ethernet and IP pseudowire SAPs (Epipe and Ipipe), VPLS SAPs, VPRN SAPs, and IES SAPs
  - ingress of IES in-band management SAPs
  - egress of VPRN and IES SAPs
  - egress of VPLS SAPs (Ethernet only)
- SDPs
  - ingress of VPLS SDPs (spoke and mesh)
  - ingress of VPRN and IES spoke SDPs

IPv6 filters can be applied at:

- network interfaces
  - ingress and egress of Ethernet network interfaces (with null or dot1q encapsulation)
  - ingress and egress of network interfaces on the 4-port OC3/STM1 Clear Channel Adapter card (with POS encapsulation)
- SAPs
  - ingress and egress of IES SAPs
  - ingress and egress of VPRN SAPs
  - ingress and egress of VPLS SAPs
- SDPs
  - ingress of VPRN spoke SDPs

– ingress of VPLS SDPs

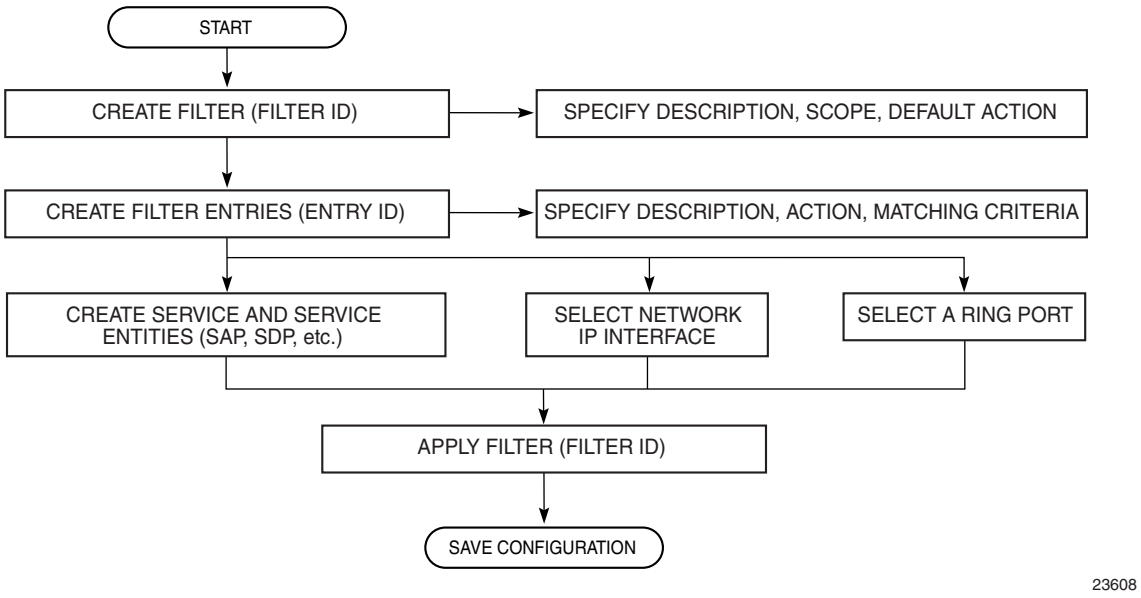
MAC filter policies can be applied at the ingress of VPLS SAPs (Ethernet, and ATM on clear channel OC3 adapter cards) and SDPs (spoke and mesh).

VLAN filters can only be applied to ring ports on the 2-port 10GigE (Ethernet) Adapter card and 2-port 10GigE (Ethernet) module.

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

Figure 13 shows the process to create filter policies and apply them to a network interface.

Figure 13 **Creating and Applying Filter Policies**



5.1.6.2 Packet Matching Criteria

IPv4 and IPv6 filter entries can specify one or more matching criteria. However, in order to support the maximum 256 entries for IPv4 or IPv6 filters, any entry that uses source port (**src-port**) and/or destination port (**dst-port**) ranges (**lt**, **gt**, or **range** keywords) as match criteria must be within the first 64 entries.

For IPv6 filters, the combined number of fields for all entries in a filter must not exceed 16 fields (or 256 bits), where a field contains the bit representation of the matching criteria.

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 the action defined in the entry is executed (that is, packets that match the criteria are either dropped or forwarded). If no match is found, the default action is to drop the packet.

Matching criteria for IP filters, MAC filters, and VLAN filters are described in Table 73, Table 74, and Table 75, respectively.

IP Filter Matching Criteria

IPv4 and IPv6 filter policies compare the matching criteria to traffic at a network interface. Matching criteria to drop or forward IP traffic are described in Table 73.

Table 73 **IP Filter Policy Criteria**

Criteria	Description
Protocol identifier/ next header	For IPv4, entering a protocol identifier allows the filter to match the IP protocol. Common protocol numbers include ICMP(1), TCP(6), and UDP(17). For a full list of protocol numbers, see the **config>filter>ip-filter>entry>match** command in the Filter Command Reference. For IPv6, entering a next header allows the filter to match the first next header following the IPv6 header.
DSCP name	Entering a DSP name allows the filter to match DiffServ Code Point (DSCP) names
Destination IP address and mask	Entering a destination IP address and mask allows the filter to match destination IP address and mask values (for IPv4) and matching destination IP address and prefix length (for IPv6). The IPv4 address scheme consists of 32 bits expressed in dotted-decimal notation. The IPv6 address scheme consists of 128 bits expressed in colon-hexadecimal format.
Destination port/range	Entering a destination port/range allows the filter to match TCP or UDP values
Fragmentation	Entering a fragment allows the filter to match the fragmentation state of packets (fragmented or non-fragmented) (not applicable to IPv6)
ICMP code	Entering an ICMP code allows the filter to match an ICMP code in the ICMP header
ICMP type	Entering an ICMP type allows the filter to match an ICMP type in the ICMP header
IP option	Entering an IP option allows the filter to match an option or range of options in the IP header (not applicable to IPv6)

Table 73 **IP Filter Policy Criteria (Continued)**

Criteria	Description
Multiple IP options	Entering multiple IP options allows the filter to match the state of multiple option fields in the IP header (true or false) (not applicable to IPv6)
Option present	Entering option present allows the filter to match the state of the option field in the IP header (present or absent) (not applicable to IPv6)
Source IP address and mask	Entering a source IP address and mask allows the filter to match a source IP address and mask values (for IPv4) or a source IP address and prefix length (for IPv6). The IPv4 address scheme consists of 32 bits expressed in dotted-decimal notation. The IPv6 address scheme consists of 128 bits expressed in colon-hexadecimal format.
Source port/range	Entering a source port/range allows the filter to match a TCP or UDP port and range values
TCP ACK	Entering TCP ACK allows the filter to match the state of the ACK bit set in the control bits of the TCP header of an IP packet (set or not set)
TCP SYN	Entering a TCP SYN allows the filter to match the state of the SYN bit set in the control bits of the TCP header of an IP packet (set or not set)

MAC Filter Matching Criteria

MAC filter policies compare the matching criteria to traffic at the ingress of a VPLS SAP or SDP (spoke or mesh). Matching criteria to drop or forward MAC traffic are described in Table 74.

Table 74 **MAC Filter Policy Criteria**

Criteria	Description
Frame type	Entering the frame type allows the filter to match a specific type of frame format; for example, Ethernet-II will match only Ethernet-II frames
Source MAC address	Entering the source MAC address allows the filter to search for a matching source MAC address. Enter the source MAC address in the form xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx; for example, 00:dc:98:1d:00:00.
Destination MAC address	Entering the destination MAC address allows the filter to search for a matching destination MAC address. Enter the destination MAC address in the form xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx; for example, 02:dc:98:1d:00:01.

Table 74 **MAC Filter Policy Criteria (Continued)**

Criteria	Description
Ethertype	Entering an Ethernet type II Ethertype value allows the value to be used as a filter match criterion. The Ethernet type field is a 2-byte field used to identify the protocol carried by the Ethernet frame. The Ethertype accepts decimal, hex, or binary in the range of 1536 to 65535.

VLAN Filter Matching Criteria

VLAN filter policies compare the matching criteria to traffic at the ingress of a ring port on the 2-port 10GigE (Ethernet) Adapter card and 2-port 10GigE (Ethernet) module. Matching criteria to drop or forward traffic are described in Table 75.

Table 75 **VLAN Filter Policy Criteria**

Criteria	Description
VLAN ID or VLAN range	Entering a VLAN identifier or range allows the filter to match VLAN ID values
Untagged	Selecting untagged allows the filter to match on Ethernet frames with no tag or dot1q header. Having no tag or dot1q header is also referred to as null encapsulation.

5.1.6.3 Ordering Filter Entries

When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Filter matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.

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

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

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

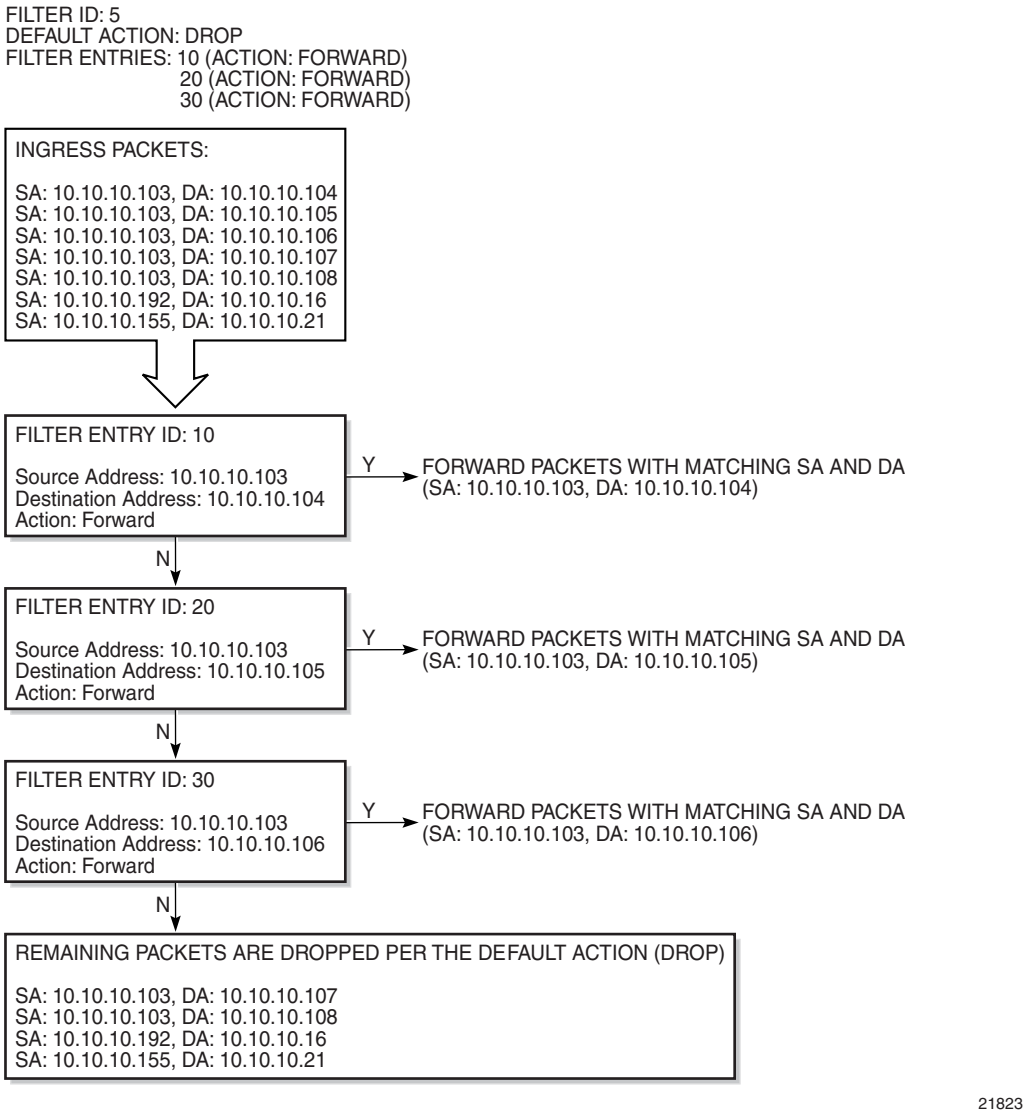
If a filter policy contains two or more entries, packets are compared in ascending entry ID order (for example, 1, 2, 3 or 10, 20, 30).

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

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

Figure 14 displays an example of several packets forwarded upon matching the filter criteria and several packets traversing through the filter entries and then dropped.

Figure 14 **Filtering Process Example**



5.1.7 Filter Log Files

Filter entries can be configured to be written to a filter log file. The log file must exist before any entries can be logged. To create a log file, use the **config**>**filter**>**log** *log-id* **create** command. Filter logs can be sent to either memory or an existing syslog server. See Filter Logs for more information.

The 7705 SAR supports filter logging for the following filters:

- ingress spoke SDP IPv4, IPv6, or MAC filters (VPLS only)
- ingress mesh SDP IPv4, IPv6, or MAC filters (VPLS only)
- ingress spoke SDP IPv4 or IPv6 filters (VPRN)

The 7705 SAR does not support filter logging for VLAN filters.

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

5.2 Configuration Notes

The following information describes the conditions for filter policy implementation.

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

See the following sections for specific notes on:

- IP Filters
- IPv6 Filters
- MAC Filters
- VLAN Filters
- Filter Logs

5.2.1 IP Filters

- Define filter entry packet matching criteria — if a filter policy is created with an entry and an 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** keyword must be specified for the entry to be active. Any filter entry without an **action** keyword specified is considered incomplete and will be inactive.

5.2.2 IPv6 Filters

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

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

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

5.2.3 MAC Filters

- If a MAC filter policy is created with an entry and entry action specified but the packet matching criteria is not defined, then all packets processed through this filter policy entry will pass and take the action specified. There are no default parameters defined for matching criteria.
- MAC filters cannot be applied to network interfaces, routable VPRN or IES services.
- Some of the MAC match criteria fields are exclusive to each other, based on the type of Ethernet frame. Use Table 76 to determine the exclusivity of fields.

Table 76 **MAC Match Criteria Exclusivity Rules**

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

5.2.4 VLAN Filters

- VLAN filters are applied to physical ring ports on the 2-port 10GigE (Ethernet) Adapter card and 2-port 10GigE (Ethernet) module. VLAN filters are exclusive to the ring adapter card and module.
- Only one VLAN filter is allowed per ingress ring port.
- The same VLAN filter can be applied to both ring ports.
- The forwarding action sends packets to the other ring port or to the v-port, depending on the packet's destination.
- The 7705 SAR does not support filter logging or statistics collection for VLAN filters.

5.2.5 Filter Logs

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

5.2.6 Reference Sources

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

5.3 Configuring Filter Policies with CLI

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

Topics in this section include:

- Basic Configuration
- Common Configuration Tasks
- Filter Management Tasks

5.4 Basic Configuration

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

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

The most basic IP exception filter policy must have the following:

- an exception filter policy ID
- scope, either exclusive or template
- at least one filter entry with a specified matching criteria

5.5 Common Configuration Tasks

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

- Creating an IPv4 or IPv6 Filter Policy
- Creating a MAC Filter Policy
- Creating a VLAN Filter Policy
- Creating a Bypass Policy for a Firewall in a Layer 2 Service
- Creating an IP Exception Filter Policy
- Configuring Filter Log Policies
- Configuring a NAT Security Profile
- Configuring a NAT Security Policy
- Applying IP and MAC Filter Policies to a Service
- Applying IP Filter Policies to Network Interfaces
- Applying VLAN Filter Policies to a Ring Port
- Creating a Match List for Filter Policies

5.5.1 Creating an IPv4 or IPv6 Filter Policy

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

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

5.5.1.1 IP Filter Policy

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

CLI Syntax:

```
config>filter# ip-filter filter-id [create]
   description description-string
   scope {exclusive | template}
```

```
default-action {drop | forward}
```

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

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

Example:
```
config>filter# ipv6-filter 10 create
config>filter# description "ipv6-filter"
config>filter# scope template
```

The following example displays a template filter policy configuration.

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

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

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

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

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

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

The following example displays an exclusive filter policy configuration.

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

5.5.1.2 IP Filter Entry

Within a filter policy, configure filter entries that contain criteria against which ingress, egress, and network traffic is matched. The action specified in the entry determines 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 (see IP Filter Entry Matching Criteria).

The **forward next-hop** command is used to implement policy-based routing. For details, see Policy-Based Routing. Use the **indirect** keyword to identify the indirect next-hop router to which packets with matching criteria will be forwarded. The **forward fc** command is used to implement multi-field classification. For details, see Multi-field Classification (MFC).

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

CLI Syntax:

```
config>filter# ip-filter {filter-id | filter-name}
   entry entry-id
      description description-string
      action [drop]
      action forward [next-hop {ip-address | indirect ip-
         address}] [fc fc-name [priority low | high]]
```

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$ action drop
config>filter>ip-filter>entry# exit
```

CLI Syntax:
```
config>filter# ip-filter {filter-id | filter-name}
   entry entry-id
      description description-string
      action {drop | forward}]
```

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

The following example displays an IP filter entry configuration.

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

5.5.1.3 IP Filter Entry Matching Criteria

Note: IPv4 and IPv6 filter entries can specify one or more matching criteria. However, in order to support the maximum 256 entries for IPv4 or IPv6 filters, any entry that uses source port (**src-port**) and/or destination port (**dst-port**) ranges (**lt**, **gt**, or **range** keywords) as match criteria must be within the first 64 entries.

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

CLI Syntax:
```
config>filter>ip-filter>entry#
   match
      dscp dscp-name
      dst-ip {ip-address/mask | ip-address ipv4-address-
         mask | ip-prefix-list prefix-list-name}
      dst-port {{lt | gt | eq} dst-port-number} | {range
         start end}
      fragment {true | false}
      icmp-code icmp-code
      icmp-type icmp-type
      ip-option ip-option-value [ip-option-mask]
      multiple-option {true | false}
```

```
                option-present {true | false}
                src-ip {ip-address/mask | ip-address ipv4-address-
                   mask | ip-prefix-list prefix-list-name}
                src-port {{lt | gt | eq} src-port-number} | {range
                   start end}
                tcp-ack {true | false}
                tcp-syn {true | false}
```

Example:

```
config>filter>ip-filter>entry# match
config>filter>ip-filter>entry>match# src-ip 10.10.10.10/
 8
config>filter>ip-filter>entry>match# dst-ip 10.10.10.91/
 8
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 10.10.10.91/8
                    src-ip 10.10.10.10/8
                exit
                action forward
            exit
----------------------------------------------
A:ALU-7>config>filter>ip-filter#
```

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

CLI Syntax:

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

Example:
```
config>filter>ipv6-filter>entry# match
config>filter>ipv6-filter>entry>match# src-ip
  2001:db8:a0b:12f0::1/128
config>filter>ipv6-filter>entry>match# dst-ip
  2001:db8:a0b:12f0::2/128
config>filter>ipv6-filter>entry>match# exit
```

The following example displays a matching configuration.

```
A:ALU-7>config>filter>ipv6-filter# info
----------------------------------------------
            description "ipv6-filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                match
                    dst-ip 2001:db8:a0b:12f0::2/128
                    src-ip 2001:db8:a0b:12f0::1/128
                exit
                action forward exit
```

5.5.1.4 IP Filter Entry for PBR to a System IP or Loopback Address

A PBR rule can be set up to extract packets from the data path and send them to the CSM for debugging or slow path forwarding, by having the **next-hop** point to a system IP or loopback interface of the 7705 SAR.

The extracted traffic can be rerouted to a final destination based on a RIB lookup on the CSM. The traffic is reinjected to the datapath based on the **next-hop** address.

Table 77 summarizes the queuing parameters for this functionality. These parameters are for slow path queues created for PBR and are not user-configurable.

Table 77 **PBR CSM Extraction Queue Parameters**

Parameter	Maximum Value
PIR	1500 kb/s
CIR	100 kb/s
MBS	20 (non-buffer-chained adapter cards) 80 (buffer-chained adapter cards)
CBS	8 buffers

The following syntax shows an example of extracting and reinjecting packets to a system IP address. An example for a loopback address would be similar.

CLI Syntax:
```
config>filter# ip-filter {filter-id | filter-name}
   entry entry-id
      action forward [next-hop {ip-address | indirect ip-
         address}] [fc fc-name [priority low | high]]
      match
         dscp dscp-name
```

Example:
```
config>filter# ip-filter 12
config>filter>ip-filter# entry 112 create
config>filter>ip-filter>entry$ action forward next-hop
 indirect 10.10.10.10
config>filter>ip-filter>entry# match
config>filter>ip-filter>entry>match# dscp be
config>filter>ip-filter>entry>match# exit
```

```
A:ALU-7>config>filter>ip-filter# info
----------------------------------------------
            scope exclusive
            entry 12 create
                match
                    dscp be
                exit
                action forward next-hop indirect 10.10.10.10
            exit
----------------------------------------------
A:ALU-7>config>filter>ip-filter#
```

5.5.2 Creating a MAC Filter Policy

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

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

5.5.2.1 MAC Filter Policy

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

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

Example:
```
config>filter>mac-filter 90 create
config>filter>mac-filter# description filter-west
config>filter>mac-filter# scope exclusive
config>filter>mac-filter# default-action drop
```

The following example displays an exclusive scope configuration.

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

5.5.2.2 MAC Filter Entry

Within a filter policy, configure filter entries that contain criteria against which ingress, egress, or network traffic is matched. The action specified in the entry determines 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 (see MAC Entry Matching Criteria).

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

CLI Syntax:
```
config>filter>mac-filter {filter-id | filter-name}
  entry entry-id [create]
    description description-string
    action [drop]
    action forward
    exit
```

Example:
```
config>filter>mac-filter 90
config>filter>mac-filter# entry 1 create
config>filter>mac-filter>entry# description "allow-104"
config>filter>mac-filter>entry# action drop
config>filter>mac-filter>entry# exit
```

The following example displays a MAC filter entry configuration.

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

5.5.2.3 MAC Entry Matching Criteria

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

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

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

The following example displays a filter matching configuration.

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

5.5.3 Creating a VLAN Filter Policy

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

- the filter type specified (VLAN)
- a filter policy ID
- a default action, either drop or forward
- at least one filter entry
- specified matching criteria (see VLAN Entry Matching Criteria)

5.5.3.1 VLAN Filter Policy

Use the following CLI syntax to configure a VLAN filter policy:

CLI Syntax:
```
config>filter>vlan-filter filter-id [create]
   description description-string
   default-action {drop | forward}
```

Example:
```
config>filter>vlan-filter 2 create
config>filter>vlan-filter# description VLAN_filter_2
config>filter>vlan-filter# default-action drop
```

The following example displays a VLAN filter configuration.

```
A:ALU-7>config>filter# info
----------------------------------------------
...
vlan-filter 2 create
description "VLAN_filter_2"
default-action drop
exit
----------------------------------------------
A:ALU-7>config>filter#
```

5.5.3.2 VLAN Filter Entry

Within a VLAN filter policy, configure filter entries that contain criteria against which ingress traffic on a ring port is matched. The action specified in the entry determines how the packets are handled, either dropped or forwarded. Forwarded packets are sent to the other ring port or the v-port, depending on the destination.

- Enter a filter entry ID. The system does not dynamically assign a value.
- Assign an action, either drop or forward.
- Specify matching criteria (see VLAN Entry Matching Criteria).

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

CLI Syntax:
```
config>filter>vlan-filter {filter-id | filter-name}
   entry entry-id [create]
      description description-string
      action {drop | forward}
      exit
```

Example:
```
config>filter>vlan-filter 2
config>filter>vlan-filter# entry 2 create
config>filter>vlan-filter>entry# description “drop-104”
config>filter>vlan-filter>entry# action drop
config>filter>vlan-filter>entry# exit
```

The following example displays a VLAN filter entry configuration.

```
A:sim1>config>filter# info
----------------------------------------------
        vlan-filter 2 create
             entry 2 create
                 description "drop-104"
                 match
                 action drop
                 exit
             exit
```

```
        exit
-------------------------------------------
A:sim1>config>filter#
```

5.5.3.3 VLAN Entry Matching Criteria

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

CLI Syntax:
```
config>filter>vlan-filter {filter-id | filter-name}
   entry entry-id
      match vlan {lt|gt|eq} vlan-id
      match vlan range vlan-id to vlan-id
      match untagged
```

Example:
```
config>filter>vlan-filter 2
config>filter>vlan-filter# entry 2
config>filter>vlan-filter# description drop_104
config>filter>vlan-filter>entry# match vlan eq 104
```

The following example displays a filter matching configuration.

```
A;ALU-7>config>filter# info
-------------------------------------------
        description "drop-104"
        entry 2 create
             description "drop-104"
             match vlan eq 104
             action drop
             exit
        exit
-------------------------------------------
A:ALU-7>config>filter#
```

5.5.4 Creating a Bypass Policy for a Firewall in a Layer 2 Service

Configuring and applying bypass filter policies is optional. The bypass policy must be given an ID or a name that must be unique within the system. If given a name, the system automatically assigns the first available ID number to the policy.

Use the following CLI syntax to configure a bypass policy.

CLI Syntax:
```
config>security>bypass bypass-id | name [create]
   entry entry-id [create]
      match [protocol protocol-id]
```

```
dst-port {lt | gt | eq} dst-port-number
dst-pot range dst-port-number dst-port-number
src-port {lt | gt | eq} src-port-number
src-port range src-port-number src-port-number
```

Example:
```
config>security>bypass 5 create
config>security>bypass# description "Sample Bypass
 Filter"
config>security>bypass# entry 1 create
config>security>bypass>entry# description "Sample Entry"
config>security>bypass>entry# match protocol "pim"
config>security>bypass>entry# exit
```

The following example displays a bypass filter configuration.

```
-----------------------------------------------
*A:Sar8 Dut-A>conf>security>bypass# info
-----------------------------------------------
    name "5"
    description "Sample Bypass Filter"
       entry 1 create
           description "Sample Entry"
           match protocol 103
       exit
-----------------------------------------------
*A:Sar8 Dut-A>conf>security>bypass#
```

5.5.5 Creating an IP Exception Filter Policy

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

- an exception filter policy ID
- scope specified, either exclusive or template
- at least one filter entry with matching criteria specified

5.5.5.1 IP Exception Filter Policy

Use the following CLI syntax to create an IP exception filter policy:

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

Example:
```
config>filter# ip-exception 1 create
config>filter>ip-except# description "IP-exception"
config>filter>ip-except# scope template
```

The following example displays a template IP exception filter policy configuration.

```
A:ALU-7>config>filter# info
----------------------------------------------
...
        ip-exception 1 create
            description "IP-exception"
            scope template
        exit
...
----------------------------------------------
A:ALU-7>config>filter#
```

5.5.5.2 IP Exception Entry Matching Criteria

Within an exception filter policy, configure exception entries that contain criteria against which ingress, egress, and network traffic is matched. Packets that match the entry criteria are allowed to transit the NGE domain in clear text.

- Enter an exception filter entry ID. The system does not dynamically assign a value.
- Specify matching criteria.

Use the following CLI syntax to configure IP exception filter matching criteria:

CLI Syntax:
```
config>filter# ip-exception filter-id
   entry entry-id [create]
      description description-string
      match
         dst-ip {ip-address/mask | ip-address ipv4-
            address-mask | ip-prefix-list prefix-list-
            name}
         dst-port {lt | gt | eq} dst-port-number
         dst-port range dst-port-number dst-port-number
         icmp-code icmp-code
         icmp-type icmp-type
         src-ip {ip-address/mask | ip-address ipv4-
            address-mask | ip-prefix-list prefix-list-
            name}
         src-port {lt | gt | eq} src-port-number
         src-port range src-port-number src-port-number
```

Example:
```
config>filter>ip-except# entry 1 create
config>filter>ip-except>entry# match
config>filter>ip-except>entry>match# src-ip 10.10.10.10/
 8
config>filter>ip-except>entry>match# dst-ip 10.10.10.91/
 8
config>filter>ip-except>entry>match# exit
```

The following example displays a matching configuration.

```
A:ALU-7>config>filter>ip-exception# info
----------------------------------------------
            description "exception-main"
            scope exclusive
            entry 1
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.10.10/8
                exit
            exit
----------------------------------------------
A:ALU-7>config>filter>ip-except#
```

5.5.6 Configuring Filter Log Policies

Use the following CLI syntax to configure filter log policy:

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

The following example displays a filter log configuration.

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

5.5.7 Configuring a NAT Security Profile

To configure NAT, you must first:

- configure a NAT security profile and policy in the **config>security** context
  - in the **config>security>profile** context, specify the timeouts for the tcp/udp/icmp protocols. This step is optional. If you do not configure the profile, a default profile is assigned.
  - in the **config>security>policy** context, configure a NAT security policy, and specify the match criteria and the action to be applied to a packet if a match is found
- then configure a NAT zone and apply the policy ID to the zone

To configure a NAT security profile, you must create the profile ID. Once created, the profile ID is referenced when you set up a NAT policy.

CLI Syntax:

```
config>security# profile profile-id [create]
   description description-string
   name profile-name
   timeouts
      icmp-request minutes seconds
      tcp-established days hours minutes seconds
      tcp-syn days hours minutes seconds
      tcp-time-wait minutes seconds
      tcp-transitory days hours minutes seconds
      udp days hours minutes seconds
      udp-dns days hours minutes seconds
      udp-initial minutes seconds
```

The following example displays a profile configuration.

Example:

```
config>security# begin
config>security# session-high-wmark 90
config>security# session-low-wmark 70
config>security# profile 2 create
config>security>profile# name "default"
config>security>profile# description "session timer
 check"
config>security>profile# timeouts
config>security>profile>timeouts# icmp-request sec 59
config>security>profile>timeouts# tcp-time-wait min 1
config>security>profile>timeouts# exit
config>security>profile# exit
config>security# commit
```

The following output displays a modified NAT profile.

```
A:ALU-7>config>security# info
----------------------------------------------
..
            session-high-wmark 90
            session-low-wmark 70
            profile 2 create
                 name "default"
                 description "For session timer check"
                 timeouts
                 exit
            exit
..
----------------------------------------------
A:ALU-7>config>security#
```

5.5.8 Configuring a NAT Security Policy

To configure NAT, you must first:

- configure a NAT security profile and policy in the **config>security** context
  - in the **config>security>profile** context, specify the timeouts for the tcp/udp/icmp protocols. This step is optional. If you do not configure the profile, a default profile is assigned.
  - in the **config>security>policy** context, configure a NAT security policy, and specify the match criteria and the action to be applied to a packet if a match is found
- then configure a NAT zone and apply the policy ID to the zone

To configure a NAT policy, you must create the policy ID.

CLI Syntax:

```
config>security# policy policy-id [create]
   description description-string
   entry entry-id [create]
      description description-string
      match [local] protocol protocol-id
         direction {zone-outbound | zone-inbound | both}
         dst-ip ip-address to ip-address
         dst-port {lt | gt | eq} port range start end
         icmp-code icmp-code
         icmp-type icmp-type
         src-ip ip-address to ip-address
         src-port {lt | gt | eq} port range start end
      action {forward | reject | nat}
      action nat [destination ip-address port tcp-udp-
         port]
```

```
      limit
        concurrent-sessions number
      profile profile-id | profile-name
    name policy-name
```

For the **action nat** command, **destination** *ip-address* and **port** *tcp-udp-port* parameters apply only to static destination NAT (port forwarding).

The following example displays a policy configuration for source NAT.

```
config>security# begin
config>security# policy 1 create
config>security>policy# name "inbound policy"
config>security>policy# description "common egress
 policy"
config>security# entry 1 create
config>security>policy>entry# description "Source NAT"
config>security>policy>entry# match
config>security>policy>entry>match# direction zone-
 inbound
config>security>policy>entry>match# exit
config>security>policy>entry># limit
config>security>policy>entry># exit
config>security>policy>entry># action nat
config>security>policy>entry># profile 2
config>security>policy>entry># exit
config>security>policy># exit
config>security># commit
```

The following example displays a policy configuration for static destination NAT.

```
config>security# begin
config>security# policy 1 create
config>security# entry 2 create
config>security>policy>entry# description "Dest NAT"
config>security>policy>entry# match local protocol udp
config>security>policy>entry>match# dst-port eq 4000
config>security>policy>entry>match# exit
config>security>policy>entry># limit
config>security>policy>entry># exit
config>security>policy>entry># action nat destination
 198.51.100.1 port 4000
config>security>policy>entry># profile 2
config>security>policy>entry># exit
config>security>policy># exit
config>security># commit
```

The following output displays a modified NAT policy output.

```
A:ALU-7>config>security# info
----------------------------------------------
..
            policy 1 create
               name "inbound policy"
               description "common egress policy"
               entry 1 create
                  description "Source NAT"
                  match
                     direction zone-inbound
                  exit
                  limit
                  action nat
                  profile 2
               exit
               entry 2 create
                  description "Dest NAT"
                  match local protocol udp
                     dst-port eq 4000
                  exit
                  limit
                  action nat destination 198.51.100.1 port 4000
                  profile 2
            exit
            commit
..
----------------------------------------------
A:ALU-7>config>security#
```

5.5.9 Applying IP and MAC Filter Policies to a Service

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

The following CLI syntaxes show how to apply filter policies to services. Use the first CLI syntax to apply an IP or MAC filter policy to a VPLS SAP, mesh SDP, or spoke SDP. Use the second CLI syntax for Epipe or Ipipe services. Use the third CLI syntax for VPRN or IES interface SAPs and spoke SDPs. (For IES SAPs, IPv6 ingress and egress filters can also be applied.)

CLI Syntax:

```
config>service# vpls service-id
   sap sap-id
      egress
         filter ip ip-filter-id
         filter ipv6 ipv6-filter-id
         filter mac mac-filter-id
      ingress
         filter ip ip-filter-id
         filter ipv6 ipv6-filter-id
```

```
        filter mac mac-filter-id
    mesh-sdp sdp-id:vc-id [vc-type {ether | vlan}]
      ingress
        filter ip ip-filter-id
        filter ipv6 ipv6-filter-id
    spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}]
      ingress
        filter ip ip-filter-id
        filter ipv6 ipv6-filter-id
```

CLI Syntax:

```
config>service# epipe service-id
  sap sap-id
    ingress
      filter ip ip-filter-id
```

CLI Syntax:

```
config>service# vprn service-id
  interface ip-int-name
    sap sap-id
      egress
        filter ip ip-filter-id
        filter ipv6 ipv6-filter-id
      ingress
        filter ip ip-filter-id
        filter ipv6 ipv6-filter-id
    spoke-sdp sdp-id:vc-id
      ingress
        filter ip ip-filter-id
        filter ipv6 ipv6-filter-id
```

The following example is for VPLS. A VPRN example includes the **interface** command (**config>service>vprn>interface**).

Example:

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

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

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

5.5.10 Applying IP Filter Policies to Network Interfaces

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

IPv4 filters are supported on all ingress and egress network interfaces. IPv6 filters are supported on all Ethernet ingress and egress network interfaces (with null or dot1q encapsulation) and on ingress and egress interfaces on the 4-port OC3/STM1 Clear Channel Adapter card (with POS encapsulation).

Filter policies must be created before they can be applied to a network interface. Create filter policies in the **config>filter** context.

CLI Syntax:

```
config>router# interface ip-int-name
   egress
     filter ip ip-filter-id
     filter ipv6 ipv6-filter-id
   ingress
     filter ip ip-filter-id
     filter ipv6 ipv6-filter-id
```

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

```
A:ALU-48>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
...
        interface "to-104"
            address 10.10.10.0/8
            port 1/1/1
            ingress
                filter ip 10
            exit
        exit
...
#------------------------------------------
A:ALU-48>config>router#
```

5.5.11 Applying VLAN Filter Policies to a Ring Port

VLAN filter policies can be applied to a ring port on the 2-port 10GigE (Ethernet) Adapter card and 2-port 10GigE (Ethernet) module. The filter operates on ingress traffic. Filter policies must be created before they can be applied. Create filter policies in the **config>filter** context.

CLI Syntax: `config>port>ethernet# vlan-filter` *`filter-id`*

Example:
```
config>port>ethernet# vlan-filter 2
```

```
A:ALU-48>config>port>ethernet# info
#------------------------------------------
...
        vlan-filter 2
...
#------------------------------------------
A:ALU-48>config>port>ethernet#
```

5.5.12 Creating a Match List for Filter Policies

IP filter policies support the use of match lists as a single match criterion. To create a match list, you must:

- specify the type of match list (for example, an IPv4 address prefix list)
- define a unique match list name (for example, “IPv4PrefixDenylist”)
- specify at least one valid IPv4 or IPv6 address prefix

Optionally, a description can also be defined.

The following example shows an IPv4 address prefix list configuration and its use in an IPv4 filter policy:

```
*A:ala-48>config>filter# info
----------------------------------------------
      match-list
        ip-prefix-list "IPv4PrefixDenylist"
           description "default IPv4 prefix denylist"
           prefix 10.0.0.0/21
           prefix 10.254.0.0/24
        exit
     exit
     ip-filter 10
        scope template
        filter-name "IPv4PrefixDenylistFilter"
        entry 10
           match
              src-ip ip-prefix-list IPv4PrefixDenylist
           exit
           action drop
        exit
      exit
----------------------------------------------
```

5.6 Filter Management Tasks

This section discusses the following filter policy management tasks:

- Renumbering Filter Policy Entries
- Modifying an IP Filter Policy
- Modifying a MAC Filter Policy
- Modifying a VLAN Filter Policy
- Removing and Deleting a Filter Policy

5.6.1 Renumbering Filter Policy Entries

The 7705 SAR 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, MAC, and VLAN filter entries:

CLI Syntax:
```
config>filter
  ip-filter {filter-id | filter-name}
    renum old-entry-id new-entry-id
```

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

CLI Syntax:
```
config>filter
  ipv6-filter {ipv6-filter-id | filter-name}
    renum old-entry-id new-entry-id
```

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

CLI Syntax:
```
config>filter
  mac-filter {filter-id | filter-name}
    renum old-entry-id new-entry-id
```

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

CLI Syntax: config>filter
vlan-filter {*filter-id* | *filter-name*}
renum *old-entry-id new-entry-id*

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

The following output displays the original IPv4 filter entry order followed by the reordered filter entries:

```
A:ALU-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.10.10/8
                exit
                action forward
            exit
            entry 30 create
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.0.100/8
                exit
                action drop
            exit
            entry 35 create
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.0.200/8
                exit
                action forward
            exit
            entry 40 create
                match
                    dst-ip 10.10.10.0/8
                    src-ip 10.10.10.106/8
                exit
                action drop
            exit
        exit
...
----------------------------------------------
A:ALU-7>config>filter#
```

```
A:ALU-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "filter-main"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.0/8
                    src-ip 10.10.10.106/8
                exit
                action drop
            exit
            entry 15 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.0.10/8
                exit
                action forward
            exit
            entry 35 create
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.10.200/8
                exit
                action forward
            exit
            entry 40 create
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.0.100/8
                exit
                action drop
            exit
        exit
...
----------------------------------------------
A:ALU-7>config>filter#
```

5.6.2 Modifying an IP Filter Policy

To access a specific IPv4 or IPv6 filter, you must specify the filter ID or the filter name (if a filter name is configured). Use the **no** form of the command to remove the command parameters or return the parameter to the default setting.

Example:

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

```
config>filter>ip-filter>entry# exit
config>filter>ip-filter#
```

Example:

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

The following output displays a modified IPv4 filter output.

```
A:ALU-7>config>filter# info
----------------------------------------------
..
        ip-filter 11 create
            description "New IP filter info"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.0/8
                    src-ip 10.10.10.106/8
                exit
                action drop
            exit
            entry 2 create
                description "new entry"
                match
                    dst-ip 10.10.10.104/8
                exit
                action drop
            exit
            entry 15 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.10.10/8
                exit
                action forward
            exit
            entry 35 create
                match
                    dst-ip 10.10.10.91/8
                    src-ip 10.10.0.200/8
                exit
                action forward
            exit
        exit
..
----------------------------------------------
A:ALU-7>config>filter#
```

5.6.3 Modifying a MAC Filter Policy

To access a specific MAC filter, you must specify the filter ID or the filter name (if a filter name is configured). Use the **no** form of the command to remove the command parameters or return the parameter to the default setting. The example below changes the action to forward.

Example:
```
config>filter# mac-filter 90
config>filter>mac-filter# description "Mac_filter90"
config>filter>mac-filter# entry 1
config>filter>mac-filter>entry# description
 "Mac_entry90_1"
config>filter>mac-filter>entry# action forward
config>filter>mac-filter>entry# exit
```

The following output displays the modified MAC filter output:

```
A:ALU-7>config>filter# info
----------------------------------------------
...
         mac-filter 90 create
              description "Mac_filter90"
              scope exclusive
              entry 1 create
                  description "Mac_entry90_1"
                  match
                       src-mac 00:dc:98:1d:00:00
                       dst-mac 02:dc:98:1d:00:01
                  exit
                  action forward
              exit
         exit
...
----------------------------------------------
A:ALU-7>config>filter#
```

5.6.4 Modifying a VLAN Filter Policy

To access a specific VLAN filter, you must specify the filter ID or the filter name (if a filter name is configured). Use the **no** form of the command to remove the command parameters or return the parameter to the default setting. The example below adds entry 65535.

Example:
```
config>filter# vlan-filter 2
config>filter>vlan-filter# entry 65535 create
config>filter>vlan-filter>entry# description
 "entry_65535"
config>filter>vlan-filter>entry# action forward
```

```
config>filter>vlan-filter>entry# match vlan range 2000
 to 3000
config>filter>vlan-filter>entry# exit
```

The following output displays the modified VLAN filter output:

```
*A:7705custDoc:Sar18>config>filter>vlan-filter# info
----------------------------------------------
    description "VLAN_filter_2"
    entry 2 create
        description "vlan_fltr_entry2"
        action forward
        match vlan eq 104
    exit
    entry 65535 create
        description "entry_65535"
        action forward
        match vlan range 2000 to 3000
    exit
----------------------------------------------
*A:7705custDoc:Sar18>config>filter>vlan-filter#
```

5.6.5 Removing and Deleting a Filter Policy

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

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

- Removing a Filter from a Service
- Removing a Filter from a Network Interface
- Removing a Filter from a Ring Port
- Deleting a Filter

5.6.5.1 Removing a Filter from a Service

To remove an IP or MAC filter from a VPLS SAP or VPLS SDP (spoke or mesh), use the first CLI syntax (below). For a VPRN or IES interface SAP or spoke SDP, use the second CLI syntax:

CLI Syntax:

```
config>service# vpls service-id
   sap sap-id
      egress
        no filter ip ip-filter-id
        no filter ipv6 ipv6-filter-id
```

```
      ingress
        no filter [ip ip-filter-id | ipv6 ipv6-filter-id
          | mac mac-filter-id]
    spoke-sdp sdp-id:vc-id
      ingress
        no filter [ip ip-filter-id | ipv6 ipv6-filter-id
          | mac mac-filter-id]
    mesh-sdp sdp-id:vc-id
      ingress
        no filter [ip ip-filter-id | ipv6 ipv6-filter-id
          | mac mac-filter-id]
```

CLI Syntax:

```
config>service# vprn service-id
  interface ip-int-name
    sap sap-id
      egress
        no filter [ip ip-filter-id | ipv6 ipv6-filter-
          id ]
      ingress
        no filter [ip ip-filter-id | ipv6 ipv6-filter-
          id ]
    spoke-sdp sdp-id:vc-id
      ingress
        no filter [ip ip-filter-id | ipv6 ipv6-filter-
          id ]
```

The following example is for VPLS. A VPRN example includes the **interface** command (**config>service>vprn>interface**).

Example:

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

5.6.5.2 Removing a Filter from a Network Interface

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

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

Example:
```
config>router# interface b11
config>router>if# egress
config>filter>if>egress# no filter ip 12
config>router>if>egress# exit
config>filter>if>#  ingress
config>filter>if>ingress# no filter ip 2
config>filter>if>ingress# exit
```

5.6.5.3 Removing a Filter from a Ring Port

To remove a VLAN filter from a ring port, enter the following CLI command. Including filter-id is optional because only one filter can be applied to a port.

CLI Syntax:
```
config>port>ethernet# no vlan-filter [filter-id]
```

Example:
```
config>port>ethernet# no vlan-filter 2
```

5.6.5.4 Deleting a Filter

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

CLI Syntax:
```
config>filter# no ip-filter {filter-id | filter-name}
```

CLI Syntax:
```
config>filter# no ipv6-filter {ipv6-filter-id | filter-
  name}
```

CLI Syntax:
```
config>filter# no mac-filter {filter-id | filter-name}
```

CLI Syntax: `config>filter# no vlan-filter {`*`filter-id`* | *`filter-name`*`}`

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

5.7 Filter Command Reference

5.7.1 Command Hierarchies

5.7.1.1 Configuration Commands

5.7.1.1.1 IP Filter Log Configuration Commands

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

5.7.1.1.2 IP Filter Policy Configuration Commands

```
config
    — filter
        — ip-filter filter-id [create]
        — ip-filter {filter-id | filter-name}
        — no ip-filter filter-id
            — default-action {drop | forward}
            — description description-string
            — no description
            — entry entry-id [create]
            — no entry entry-id
                — action [drop]
                — action forward [next-hop {ip-address | indirect ip-address}] [fc fc-name [priority
                    low | high]]
                — no action
                — description description-string
                — no description
                — log log-id
                — no log
                — match [protocol protocol-id]
                — no match
                    — dscp dscp-name
                    — no dscp
                    — dst-ip {ip-address/mask | ip-address ipv4-address-mask | ip-prefix-list prefix-
                        list-name}
                    — no dst-ip
```

- **dst-port** {**lt** | **gt** | **eq**} *dst-port-number*
- **dst-port range** *dst-port-number dst-port-number*
- **no dst-port**
- **fragment** {**true** | **false**}
- **no fragment**
- **icmp-code** *icmp-code*
- **no icmp-code**
- **icmp-type** *icmp-type*
- **no icmp-type**
- **ip-option** *ip-option-value* [*ip-option-mask*]
- **no ip-option**
- **multiple-option** {**true** | **false**}
- **no multiple-option**
- **option-present** {**true** | **false**}
- **no option-present**
- **src-ip** {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *prefix-list-name*}
- **no src-ip**
- **src-port** {**lt** | **gt** | **eq**} *src-port-number*
- **src-port range** *src-port-number src-port-number*
- **no src-port**
- **tcp-ack** {**true** | **false**}
- **no tcp-ack**
- **tcp-syn** {**true** | **false**}
- **no tcp-syn**

- **filter-name** *filter-name*
- **no filter-name**
- **renum** *old-entry-id new-entry-id*
- **scope** {**exclusive** | **template**}
- **no scope**

5.7.1.1.3 IPv6 Filter Policy Configuration Commands

config

- **filter**
  - **ipv6-filter** *ipv6-filter-id* [**create**]
  - **ipv6-filter** {*filter-id* | *filter-name*}
  - **no ipv6-filter** *ipv6-filter-id*
    - **default-action** {**drop** | **forward**}
    - **description** *description-string*
    - **no description**
    - **entry** *entry-id* [**create**]
    - **no entry** *entry-id*
      - **action** {**drop** | **forward**}
      - **no action**
      - **description** *description-string*
      - **no description**
      - **log** *log-id*
      - **no log**
      - **match** [**next-header** *next-header*]
      - **no match**

```
            — dscp dscp-name
            — no dscp
            — dst-ip {ipv6-address/prefix-length | ipv6-address ipv6-address-mask |
                 ipv6-prefix-list prefix-list-name}
            — no dst-ip
            — dst-port {lt | gt | eq} dst-port-number
            — dst-port range dst-port-number dst-port-number
            — no dst-port
            — icmp-code icmp-code
            — no icmp-code
            — icmp-type icmp-type
            — no icmp-type
            — src-ip {ipv6-address/prefix-length | ipv6-address ipv6-address-mask |
                 ipv6-prefix-list prefix-list-name}
            — no src-ip
            — src-port {lt | gt | eq} src-port-number
            — src-port range src-port-number src-port-number
            — no src-port
            — tcp-ack {true | false}
            — no tcp-ack
            — tcp-syn {true | false}
            — no tcp-syn
      — filter-name filter-name
      — no filter-name
      — renum old-entry-id new-entry-id
      — scope {exclusive | template}
      — no scope
```

5.7.1.1.4 MAC Filter Policy Commands

```
config
    — filter
        — mac-filter filter-id [create]
        — mac-filter {filter-id | filter-name}
        — no mac-filter filter-id
            — default-action {drop | forward}
            — description description-string
            — no description
            — entry entry-id [create]
            — no entry entry-id
                — action [drop]
                — action forward
                — no action
                — description description-string
                — no description
                — log log-id
                — no log
                — match frame-type {802dot3 | 802dot2-llc | 802dot2-snap | ethernet_II}
                — no match
                    — dst-mac ieee-address
                    — no dst-mac
```

```
            — etype 0x0600..0xffff
            — no etype
            — src-mac ieee-address
            — no src-mac
        — filter-name filter-name
        — no filter-name
        — renum old-entry-id new-entry-id
        — scope {exclusive | template}
        — no scope
```

5.7.1.1.5 VLAN Filter Policy Commands

```
config
    — filter
        — vlan-filter filter-id [create]
        — vlan-filter {filter-id | filter-name}
        — no vlan-filter filter-id
            — default-action {drop | forward}
            — description description-string
            — no description
            — entry entry-id [create]
            — no entry entry-id
                — action {drop | forward}
                — no action
                — description description-string
                — no description
                — match vlan {lt | gt | eq}  vlan-id
                — match vlan range vlan-id to vlan-id
                — match untagged
                — no match
            — filter-name filter-name
            — no filter-name
            — renum old-entry-id new-entry-id
```

5.7.1.1.6 IP Exception Filter Policy Configuration Commands

```
config
    — filter
        — ip-exception filter-id [create]
        — [no] ip-exception {filter-id | filter-name}
            — description description-string
            — no description
            — entry entry-id [create]
            — no entry entry-id
                — description description-string
                — no description
                — match [protocol protocol-id]
                — no match
```

```
            — dst-ip {ip-address/mask | ip-address ipv4-address-mask | ip-prefix-list prefix-
                list-name}
            — no dst-ip
            — dst-port {lt | gt | eq} dst-port-number
            — dst-port range dst-port-number dst-port-number
            — no dst-port
            — icmp-code icmp-code
            — no icmp-code
            — icmp-type icmp-type
            — no icmp-type
            — src-ip {ip-address/mask | ip-address ipv4-address-mask | ip-prefix-list prefix-
                list-name}
            — no src-ip
            — src-port {lt | gt | eq} src-port-number
            — src-port range src-port-number src-port-number
            — no src-port
        — filter-name filter-name
        — no filter-name
        — renum old-entry-id new-entry-id
        — scope {exclusive | template}
        — no scope
```

5.7.1.1.7 Security Policy Commands

```
config
    — security
        — abort
        — app-group {group-id | name} [create]
        — no app-group {group-id | name}
            — description description-string
            — no description
            — entry entry-id [create]
            — no entry entry-id
                — match  [protocol protocol-id]
                — no match
                    — dst-port {lt | gt | eq} port
                    — dst-port range start end
                    — no dst-port
                    — icmp-code icmp-code
                    — no icmp-code
                    — icmp-type icmp-type
                    — no icmp-type
                    — src-port {lt | gt | eq} port
                    — src-port range start end
                    — no src-port
            — name name
            — no name
        — begin
        — bypass {bypass-id | name} [create]
        — no bypass {bypass-id | name}
            — description description-string
```

- **no description**
- **entry** *entry-id* [**create**]
- **no entry** *entry-id*
  - **description** *description-string*
  - **no description**
  - **match** [**protocol** *protocol-id*]
  - **no match**
    - **dst-port** {**lt** | **gt** | **eq**} *dst-port-number*
    - **dst-port range** *dst-port-number dst-port-number*
    - **no dst-port**
    - **src-port** {**lt** | **gt** | **eq**} *src-port-number*
    - **src-port range** *src-port-number src-port-number*
    - **no src-port**
  - **name** *name*
  - **no name**
- **commit**
- **host-group** {*group-id* | *name*} [**create**]
- **no host-group** {*group-id* | *name*}
  - **description** *description-string*
  - **no description**
  - **host** *ip-address* [**to** *ip-address*]
  - **no host**
  - **name** *name*
  - **no name**
- **logging**
  - **log-id** {*log-id* | *log-name*} [**create**]
  - **no log-id** {*log-id* | *log-name*}
    - **description** *description-string*
    - **no description**
    - **destination** {**memory** [*size*] | **syslog** *syslog-id*}
    - **no destination**
    - **name** *name*
    - **no name**
    - **profile** {*logging-profile-id* | *logging-profile-name*}
    - [**no**] **shutdown**
    - [**no**] **wrap-around**
  - **profile** {*profile-id* | *profile-name*} [**create**]
  - **no profile** {*profile-id* | *profile-name*}
    - **description** *description-string*
    - **no description**
    - **event-control** *event-type* [**event** *event*] {**suppress** | **throttle** | **off**}
    - **name** *name*
    - **no name**
- **policer-group** {*group-id* | *name*} [**create**]
- **no policer-group** {*group-id* | *name*}
  - **description** *description-string*
  - **no description**
  - **name** *name*
  - **no name**
  - **rate** *rate* **cbs** *size* [**bytes** | **kilobytes**]
  - **no rate**
- **policy** {*policy-id* | *policy-name*} [**create**]
- **no policy** {*policy-id* | *policy-name*}
  - **description** *description-string*

```
— no description
— entry entry-id [create]
— no entry entry-id
    — action {forward | reject | drop | nat}
    — action nat [destination ip-address port tcp-udp-port]
    — description description-string
    — no description
    — [no] limit
        — concurrent-sessions number
        — no concurrent-sessions
        — [no] fwd-direction-only
    — logging {to log-id {log-id | name} | suppressed | to zone}
    — no logging
    — match [local] [protocol protocol-id ]
    — match [app-group {group-id | name}]
    — no match
        — direction {zone-outbound | zone-inbound | both}
        — dst-ip ip-address to ip-address
        — dst-ip host-group {group-id | name}
        — no dst-ip
        — dst-port {lt | gt | eq} port
        — 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 to ip-address
        — src-ip host-group {group-id | name}
        — no src-ip
        — src-port {lt | gt | eq} port
        — src-port range start end
        — no src-port
    — profile {profile-id | profile-name}
    — no profile
— name policy-name
— no name
— profile {profile-id | profile-name} [create]
— no profile {profile-id | profile-name}
    — application
        — alg {auto | ftp | tftp}
        — no alg
        — [no] assurance
            — dns
                — [no] reply-only
            — icmp
                — [no] limit-type3
                — request-limit packets
                — no request-limit
            — ip
                — options {permit ip-option-mask | permit-any}
                — options ip-option-name [ip-option-name]
            — tcp
                — [no] strict
```

- **description** *description-string*
- **no description**
- **fwd-policer-group** {*group-id* | *name*}
- **no fwd-policer-group**
- [**no**] **name** *profile-name*
- **rev-policer-group** {*group-id* | *name*}
- **no rev-policer-group**
- [**no**] **timeouts**
  - **icmp-request** [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
  - **no icmp-request**
  - **other-sessions** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
  - **no other-sessions**
  - **tcp-established** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
  - **no tcp-established**
  - **tcp-syn** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
  - **no tcp-syn**
  - **tcp-time-wait** [**min** *minutes*] [**sec** *seconds*]
  - **no tcp-time-wait**
  - **tcp-transitory** [**days** days] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
  - **no tcp-transitory**
  - **udp** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
  - **no udp**
  - **udp-dns** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
  - **no udp-dns**
  - **udp-initial**[**min** *minutes*] [**sec** *seconds*]
  - **no udp-initial**
- **session-high-wmark** *percentage*
- **no session-high-wmark**
- **session-low-wmark** *percentage*
- **no session-low-wmark**

5.7.1.1.8 Filter Match List Commands

config
- **filter**
  - **match-list**
    - **ip-prefix-list** *ip-prefix-list-name* [**create**]
    - **no ip-prefix-list** *ip-prefix-list-name*
      - **description** *description-string*
      - **no description**
      - [**no**] **prefix** *ip-prefix/prefix-length*
      - [**no**] **prefix-exclude** *ip-prefix/prefix-length*
    - **ipv6-prefix-list** *ipv6-prefix-list-name* [**create**]
    - **no ipv6-prefix-list** *ipv6-prefix-list-name*
      - **description** *description-string*
      - **no description**
      - [**no**] **prefix** *ipv6-prefix/prefix-length*
      - [**no**] **prefix-exclude** *ipv6-prefix/prefix-length*

5.7.1.2 Show Commands

```
show
    — filter
        — ip
        — ip ip-filter-id [detail]
        — ip ip-filter-id [associations | counters]
        — ip ip-filter-id entry entry-id counters
        — ip-exception
        — ip-exception ip-filter-id
        — ip-exception ip-filter-id [associations | counters]
        — ip-exception ip-filter-id entry entry-id counters
        — ipv6
        — ipv6 ipv6-filter-id [detail]
        — ipv6 ipv6-filter-id [associations | counters]
        — ipv6 ipv6-filter-id entry entry-id counters
        — log [bindings]
        — log log-id [match string]
        — mac {mac-filter-id [entry entry-id] [association | counters]}
        — match-list
            — ip-prefix-list [prefix-list-name]
            — ip-prefix-list prefix-list-name references
            — ipv6-prefix-list [prefix-list-name]
            — ipv6-prefix-list prefix-list-name references
        — vlan [filter-id [entry entry-id]]

show
    — security
        — app-group [group-id | name] [entry entry-id] [detail]
        — capture [format {decode | raw}]
        — control-summary
        — engine
        — host-group
        — log [log-id | name]
        — log events [type event-type]
        — log profile {log-profile-id | name} [type event-type]
        — log profiles
        — policer-group [group-id | name] [statistics]
        — policing-summary [group-id | name] [statistics]
        — policy [policy-id | name] [detail | association]
        — policy [policy-id | name] [entry entry-id] [detail | association]
        — profile [profile-id | name] [detail | association]
        — session-summary [service service-id] [router router-instance]
        — summary
        — zone [service service-id ] [router router-instance]
        — zone [zone-id | name] [detail | interface | statistics]
            — nat pool [pool-id | name] [detail]
            — policy [entry entry-id] [detail | statistics]
            — session [inbound | outbound] [forward | nat]
            — session session-id [detail | statistics]}
```

5.7.1.3 Clear Commands

clear
- **filter**
  - **ip** *ip-filter-id* [**entry** *entry-id*] [**ingress** | **egress**]
  - **ipv6** *ipv6-filter-id* [**entry** *entry-id*] [**ingress** | **egress**]
  - **log** *log-id*
  - **mac** *mac-filter-id* [**entry** *entry-id*] [**ingress** | **egress**]
- **security**
  - **session** *session-id* **statistics**
  - **zone** [*zone-id* | *name*] **statistics**
  - **zone** [*zone-id* | *name*] **sessions** [**inbound** | **outbound** | **all**]
  - **zone** [*zone-id* | *name*] **statistics**

5.7.1.4 Monitor Commands

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

5.7.2 Command Descriptions

5.7.2.1 Configuration Commands

- Generic Commands
- Filter Log Commands
- Filter Policy Commands
- General Filter Entry Commands
- IP, MAC, VLAN, and IP Exception Filter Entry Commands
- IP, MAC, and IP Exception Filter Match Criteria Commands
- Security Policy Commands

5.7.2.1.1 Generic Commands

description

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

Context config>filter>ip-exception
config>filter>ip-exception>entry
config>filter>ip-filter
config>filter>log
config>filter>ip-filter>entry
config>filter>ipv6-filter
config>filter>ipv6-filter>entry
config>filter>mac-filter
config>filter>mac-filter>entry
config>filter>match-list>ip-prefix-list
config>filter>match-list>ipv6-prefix-list
config>filter>vlan-filter
config>filter>vlan-filter>entry
config>security>app-group
config>security>bypass
config>security>bypass>entry
config>security>host-group
config>security>logging>log
config>security>logging>profile
config>security>policer-group
config>security>policy
config>security>policy>entry
config>security>profile

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 n/a

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

Context config>filter>log
config>filter>log>summary

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

5.7.2.1.2 Filter Log Commands

log

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

Context config>filter

Description This command enables the context to create a filter log policy.

The **no** form of the command deletes the filter log ID. The log cannot be deleted if there are filter entries configured to write to the log. All filter entry logging associations need to be removed before the log can be deleted.

Default log 101

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

Parameters *log-id* — the filter log ID destination expressed as a decimal integer

Values 101 to 199

destination

Syntax **destination memory** *num-entries*
destination syslog *syslog-id*
no destination

Context config>filter>log

Description This command configures the destination for filter log entries for the specified filter log ID.

Filter logs can be sent to either memory or an existing syslog server. If the filter log destination is **memory**, the maximum number of entries in the log must be specified.

The **no** form of the command deletes the filter log association.

Default no destination

Parameters *num-entries* — specifies that the destination of the filter log ID is a memory log. The *num-entries* value is the maximum number of entries in the filter log expressed as a decimal integer.

Values 1 to 50000

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

Values 1 to 10

summary

Syntax **summary**

Context config>filter>log

Description This command enables the context to configure log summarization. These settings apply only if syslog is the log destination.

summary-crit

Syntax **summary-crit dst-addr**
summary-crit src-addr
no summary-crit

Context config>filter>log>summary

Description This command defines the key of the index of the mini-table. If key information is changed while summary is in the **no shutdown** state, the filter summary mini-table is flushed and reconfigured with different key information. Log packets received during the reconfiguration time will be handled as if summary was not active.

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

Default dst-addr

Parameters **dst-addr** — specifies that received log packets are summarized based on the destination IP address

src-addr — specifies that received log packets are summarized based on the source IP address

wrap-around

Syntax [**no**] **wrap-around**

Context config>filter>log

Description This command configures a memory filter log to store log entries until full or to store the most recent log entries (circular buffer).

Specifying **wrap-around** configures the memory filter log to store the most recent filter log entries (circular buffer). When the log is full, the oldest filter log entries are overwritten with new entries.

The **no** form of the command configures the memory filter log to accept filter log entries until full. When the memory filter log is full, filter logging for the log filter ID ceases.

Default wrap-around

5.7.2.1.3 Filter Policy Commands

ip-exception

Syntax **ip-exception** *filter-id* [**create**]
[**no**] **ip-exception** {*filter-id* | *filter-name*}

Context config>filter

Description This command creates a configuration context for an IPv4 exception filter policy. After creating an exception filter ID, you can optionally assign it to a unique name with the filter-name command. The exception filter name can be used instead of the ID for exception configuration commands, show commands, monitor commands, clear commands, and port and interface association commands.

IP exception filter policies specify matching criteria that allow a packet to be an exception to where it is applied. For more information, refer to the **ip-exception** command in Router Interface Commands.

The IP exception filter policy is a template that can be applied to multiple router interface group encryption contexts as long as the **scope** of the policy is configured as **template**.

Any changes made to the existing policy, using any subcommands, are applied immediately to all network interfaces where the policy is applied.

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

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

Values 1 to 65535

filter-name — the IP exception filter policy name, up to 64 characters in length. The name must already exist within the created IP exceptions.

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

ip-filter

Syntax **ip-filter** *filter-id* [**create**]
ip-filter {*filter-id* | *filter-name*}
no ip-filter {*filter-id* | *filter-name*}

Context config>filter

Description This command creates a configuration context for an IPv4 filter policy. After creating a filter, you can optionally assign it a unique filter name with the filter-name command. The filter name can be used instead of the filter ID to refer to a filter for filter configuration commands, show commands, monitor commands, clear commands, and port association commands.

Filter IDs and filter names support CLI auto-completion. For more information, refer to the 7705 SAR Basic System Configuration Guide, “Entering CLI Commands”.

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 subcommands, will be applied immediately to all network interfaces where this policy is applied.

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

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

Values 1 to 65535

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

filter-name — the filter name, up to 64 characters in length

ipv6-filter

Syntax **ipv6-filter** *ipv6-filter-id* [**create**]
ipv6-filter {*ipv6-filter-id* | *filter-name*}
no ipv6-filter {*ipv6-filter-id* | *filter-name*}

Context config>filter

Description This command creates a configuration context for an IPv6 filter policy. After creating a filter, you can optionally assign it a unique filter name with the filter-name command. The filter name can be used instead of the filter ID to refer to a filter for filter configuration commands, show commands, monitor commands, clear commands, and port association commands.

Filter IDs and Filter names support CLI auto-completion. For more information, refer to the 7705 SAR Basic System Configuration Guide, “Entering CLI Commands”.

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 subcommands, will be applied immediately to all network interfaces where this policy is applied.

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

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

Values 1 to 65535

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

filter-name — the filter name, up to 64 characters in length

mac-filter

Syntax **mac-filter** *filter-id* [**create**]
mac-filter {*filter-id* | *filter-name*}
no mac-filter {*filter-id* | *filter-name*}

Context config>filter

Description This command enables the context for a MAC filter policy. After creating a filter, you can optionally assign it a unique filter name with the filter-name command. The filter name can be used instead of the filter ID to refer to a filter for filter configuration commands, show commands, monitor commands, clear commands, and port association commands.

Filter IDs and filter names support CLI auto-completion. For more information, refer to the 7705 SAR Basic System Configuration Guide, “Entering CLI Commands”.

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

The MAC filter policy, sometimes referred to as an access control list (ACL), is a template that can be applied to multiple services as long as the **scope** of the policy is **template**. It can also be used to refine port mirroring so that only the desired MAC addresses are mirrored.

A MAC filter policy can be applied to VPLS ingress and egress SAPs and ingress SDPs. MAC filter policies cannot be applied to a network interface, a VPRN service, or an IES service.

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

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

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

Values 1 to 65535

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

filter-name — the filter name, up to 64 characters in length

vlan-filter

Syntax **vlan-filter** *filter-id* [**create**]
vlan-filter {*filter-id* | *filter-name*}
no vlan-filter {*filter-id* | *filter-name*}

Context config>filter

Description This command enables the context for a VLAN filter policy. After creating a filter, you can optionally assign it a unique filter name with the filter-name command. The filter name can be used instead of the filter ID to refer to a filter for filter configuration commands, show commands, monitor commands, clear commands, and port association commands.

Filter IDs and Filter names support CLI auto-completion. For more information, refer to the 7705 SAR Basic System Configuration Guide, “Entering CLI Commands”.

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

The VLAN filter policy, sometimes referred to as an access control list (ACL), is a template that can be applied to ring ports on the 2-port 10GigE (Ethernet) Adapter card and 2-port 10GigE (Ethernet) module. Each ring port can support one VLAN filter, and the same VLAN filter can be applied to both ring ports. The **scope** of a VLAN policy is always **template**.

A VLAN filter policy cannot be applied to any other type of adapter card.

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

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

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

Values 1 to 65535

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

filter-name — the filter name, up to 64 characters in length

default-action

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

Context config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-filter
config>filter>vlan-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, MAC, or VLAN filter entries of the filter.

Default drop

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

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

filter-name

Syntax **filter-name** *filter-name*
no filter-name

Context config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-filter
config>filter>vlan-filter
config>filter>ip-exception

Description This command creates a unique name to associate with this filter. The filter name can be used instead of the filter ID to refer to a filter for filter configuration commands, show commands, monitor commands, clear commands, and port and interface association commands.

Parameters *filter-name* — the filter name, up to 64 characters in length

renum

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

Context config>filter>ip-exception
config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-filter
config>filter>vlan-filter

Description This command renumbers existing IP, MAC, VLAN, or IP exception filter entries to properly sequence filter entries.

This may be required in some cases since the software 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 256 (ip-exception, ip-filter, ipv6-filter, mac-filter)
1 to 64 (vlan-filter)

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

Values 1 to 256 (ip-exception, ip-filter, ipv6-filter, mac-filter)
1 to 64 (vlan-filter)

scope

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

Context config>filter>ip-exception
config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-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

5.7.2.1.4 General Filter Entry Commands

entry

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

Context config>filter>ip-exception
config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-filter
config>filter>vlan-filter

Description This command creates or edits a 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.

Filter entry IDs support CLI auto-completion. For more information, refer to the 7705 SAR Basic System Configuration Guide, “Entering CLI Commands”.

IPv4 and IPv6 filter entries can specify one or more matching criteria. However, in order to support the maximum 256 entries for IPv4 or IPv6 filters, any entry that uses source port (**src-port**) and/or destination port (**dst-port**) ranges (**lt**, **gt**, or **range** keywords) as match criteria must be within the first 64 entries. See the dst-port and src-port commands for more information.

For IPv6 filters, the combined number of fields for all entries in a filter must not exceed 16 fields (or 256 bits), where a field contains the bit representation of the matching criteria.

Some adapter cards have limitations on the size of ACLs that can be supported and therefore cannot support the maximum number of IPv6 filter entries. If you attempt to configure more entries than the card can support, the following error log event and SNMP trap are generated:

“Class MDA Module : runtime event, details: Filter <filter id> ACL_STATUS_IPV6_ FILTER_ENTRIES_EXCEEDED Config Error!”

SNMPv2-MIB:snmpTrapOID.0 : (1.3.6.1.4.1.6527.6.1.2.3.2.1.0.13 (ALU-CHASSIS-MIB:aluEqMdaCriticalRuntimeError)) Syntax: ObjectID ALU-CHASSIS-MIB:aluChassisNotifyMdaRuntimeStatusContext.0 : (runtime event, details: Filter <filter id> ACL_STATUS_IPV6_FILTER_ENTRIES_EXCEEDED Config Error!) Syntax: SNMPv2-TC:DisplayString

where <filter id> is the filter policy ID

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 are considered incomplete and are rendered inactive.

The **no** form of the command removes the specified entry from the filter. Entries removed from the filter are immediately removed from all entities to which that filter is applied.

Default n/a

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 256 (IP exception filters, IPv4 filters, IPv6 filters, and MAC filters)

1 to 64 (VLAN filters)

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

5.7.2.1.5 IP, MAC, VLAN, and IP Exception Filter Entry Commands

action

Syntax **action** [**drop**]
action forward [**next-hop** {*ip-address* | **indirect** *ip-address*}] [**fc** *fc-name* [**priority***low*| *high*]]
no action

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

Description This command specifies what action to take (drop or forward) when packets match the entry criteria. The **action** keyword must be entered for the entry to be active. If neither **drop** nor **forward** is specified, the filter action is drop.

The **action forward next-hop** keywords cannot be applied to multicast traffic and only apply to IPv4.

The **action forward fc** keywords only apply to IPv4.

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

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

Default no action

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

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

next-hop *ip-address* — specifies the IPv4 address of the direct next hop to which packets matching the entry criteria will be forwarded

indirect *ip-address* — specifies the IPv4 address of the indirect next hop to which packets matching the entry criteria will be forwarded. The direct next-hop IPv4 address and egress IP interface are determined by a route table lookup.

If the next hop is not available, then a routing lookup is performed and if a match is found then the packet will be forwarded to the result of that lookup. If no match is found, then an “ICMP destination unreachable” message is send back to the origin.

Values 0.0.0.0 to 255.255.255.255 (dotted-decimal notation)

fc *fc-name* — specifies the forwarding class (FC) to be used for queuing packets through the 7705 SAR. Each FC can be mapped to a different queue, or multiple FCs can be handled by the same queue.

There are eight forwarding classes, providing different classes of service. The forwarding classes are: nc (network control), h1 (high 1), ef (expedited forwarding), h2 (high 2), l1 (low 1), l2 (low 2), af (assured forwarding), be (best effort).

Values be, l2, af, l1, h2, ef, h1, nc

priority *low*| *high* — specifies the priority assigned to incoming traffic. Traffic priority is important for internal processes when some traffic may be dropped because of congestion. Low-priority traffic is dropped first.

action

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

Context config>filter>ipv6-filter>entry
config>filter>vlan-filter>entry

Description This command specifies what action to take (drop or forward) when packets match the entry criteria. The **action** keyword must be entered and for the entry to be active. If neither **drop** nor **forward** is specified, the filter action is drop.

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

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

Default drop

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

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

log

Syntax **log** *log-id*
no log

Context config>filter>ip-filter>entry
config>filter>ipv6-filter>entry
config>filter>mac-filter>entry

Description This command enables the context to enable filter logging for a filter entry and specifies the destination filter log ID.

The filter log ID must exist before a filter entry can be enabled to use the filter log ID.

The **no** form of the command disables logging for the filter entry.

Default no log

Parameters *log-id* — the filter log ID destination expressed as a decimal integer

Values 101 to 199

match

Syntax **match** [**protocol** *protocol-id*]
no match

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

Description This command enables the context to enter match criteria for the IPv4 or IP exception 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-id* — *protocol-number* or *protocol-name*

protocol-number — the protocol number in decimal, hexadecimal, or binary, representing the IP protocol to be used as a filter match criterion. Common protocol numbers include ICMP(1), TCP(6), and UDP(17) (see Table 78).

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — configures the protocol name representing the IP protocol to be used as a filter match criterion

Values **IPv4 filter keywords**: none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip, * - udp/tcp wildcard

IP exception filter keywords: none, icmp, igmp, tcp, udp, rsvp, ospf-igp, pim, vrrp

Table 78 **IP Protocol IDs and Descriptions**

Protocol ID	Protocol	Description
1	icmp	Internet Control Message
2	igmp	Internet Group Management
4	ip	IP in IP (encapsulation)
6	tcp	Transmission Control

Table 78 **IP Protocol IDs and Descriptions (Continued)**

Protocol ID	Protocol	Description
8	egp	Exterior Gateway Protocol
9	igp	Any private interior gateway
17	udp	User Datagram
27	rdp	Reliable Data Protocol
41	ipv6	IPv6
43	ipv6-route	Routing Header for IPv6
44	ipv6-frag	Fragment Header for IPv6
45	idrp	Inter-Domain Routing Protocol
46	rsvp	Reservation Protocol
47	gre	General Routing Encapsulation
58	ipv6-icmp	ICMP for IPv6
59	ipv6-no-nxt	No Next Header for IPv6
60	ipv6-opts	Destination Options for IPv6
80	iso-ip	ISO Internet Protocol
88	eigrp	EIGRP
89	ospf-igp	OSPFIGP
97	ether-ip	Ethernet-within-IP Encapsulation
98	encap	Encapsulation Header
102	pnni	PNNI over IP
103	pim	Protocol Independent Multicast
112	vrrp	Virtual Router Redundancy Protocol
115	l2tp	Layer Two Tunneling Protocol
118	stp	Schedule Transfer Protocol
123	ptp	Performance Transparency Protocol
124	isis	ISIS over IPv4
126	crtp	Combat Radio Transport Protocol
127	crudp	Combat Radio User Datagram

Table 78 **IP Protocol IDs and Descriptions (Continued)**

Protocol ID	Protocol	Description
132	sctp	Stream Control Transmission Protocol
137	mpls-in-ip	MPLS in IP

Note:

- PTP in the context of IP or IP exception filters is defined as Performance Transparency Protocol. IP protocols can be used as IP or IP exception filter match criteria; the match is made on the 8-bit protocol field in the IP header.
- PTP in the context of SGT QoS is defined as Precision Timing Protocol and is an application in the 7705 SAR. The PTP application name is also used in areas such as event-control and logging. Precision Timing Protocol is defined in IEEE 1588-2008.

match

Syntax **match** [**next-header** *next-header*]
no match

Context config>filter>ipv6-filter>entry

Description This command enables the context to enter match criteria for the IPv6 filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.

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 *next-header* — *protocol-number* or *protocol-name*

protocol-number — the protocol number in decimal, hexadecimal, or binary, representing the IP protocol to be used as the IPv6 next header filter match criterion This parameter is similar to the **protocol** parameter used in IPv4 filter match criteria. See Table 78 for a list of common protocol numbers.

Values [1 to 42 | 45 to 49 | 52 to 59 | 61 to 255]D
[0x0 to 0x2A | 0x2D to 0x31 | 0x34 to 0x3B | 0x3D to 0xFF]H
[0b0 to 0b101010 | 0b101101 to 0b110001 | 0b110100 to 0b111011 | 0b111101 to 0b11111111]B

protocol-name — the protocol name to be used as the IPv6 next header filter match criterion. This parameter is similar to the **protocol** parameter used in IPv4 filter match criteria. See Table 78 for a list of common protocol numbers.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip, * - udp/tcp wildcard

match

Syntax **match frame-type** {**802dot3** | **802dot2-llc** | **802dot2-snap** | **ethernet_II**}
no match

Context config>filter>mac-filter>entry

Description This command enables the context for entering/editing match criteria for the filter entry and specifies an Ethernet frame type for the entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.

If more than one match criterion (within one match statement) is configured, then all criteria must be satisfied (AND function) before the action associated with the match will be executed.

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*.

Default frame-type 802dot3

Parameters **frame-type** — configures an Ethernet frame type to be used for the MAC filter match criteria

802dot3 — specifies the frame type as Ethernet IEEE 802.3

802dot2-llc — specifies the frame type as Ethernet IEEE 802.2 LLC

802dot2-snap — specifies the frame type as Ethernet IEEE 802.2 SNAP

ethernet_II — specifies the frame type as Ethernet Type II

match

Syntax **match vlan** {**lt** | **gt** | **eq**} *vlan-id*
match vlan range *vlan-id* **to** *vlan-id*
match untagged
no match

Context config>filter>vlan-filter>entry

Description This command accesses the match criteria for the filter entry and specifies a match criteria. If the match criteria are satisfied, the action associated with the match criteria is executed.

Only one match criterion (within one match statement) is allowed.

The **no** form of the command removes the match criteria for the *entry-id*.

Default no match

Parameters **vlan** {**lt** | **gt** | **eq**} *vlan-id* — specifies an operator and a *vlan-id* to be used for the VLAN filter match criteria (**lt** for less than, **gt** for greater than, and **eq** for equal to)

Values 1 to 4094

vlan range *vlan-id* **to** *vlan-id* — specifies a range of VLAN IDs to be used for the VLAN filter match criteria.

Values 1 to 4094

untagged — specifies that Ethernet frames with no tag or dot1q header (null encapsulation) are used for the VLAN filter match criteria

5.7.2.1.6 IP, MAC, and IP Exception Filter Match Criteria Commands

dscp

Syntax **dscp** *dscp-name*
no dscp

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion.

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

Default no dscp

Parameters *dscp-name* — a DSCP name that has been previously mapped to a value using the **dscp-name** command. The DiffServ Code Point may only be specified by its name.

Values be | cp1 | cp2 | cp3 | cp4 | cp5 | cp6 | cp7 | cs1 | cp9 | af11 | cp11 | af12 | cp13 | af13 | cp15 | cs2 | cp17 | af21 | cp19 | af22 | cp21 | af23 | cp23 | cs3 | cp25 | af31 | cp27 | af32 | cp29 | af33 | cp31 | cs4 | cp33 | af41 | cp35 | af42 | cp37 | af43 | cp39 | cs5 | cp41 | cp42 | cp43 | cp44 | cp45 | ef | cp47 | nc1 | cp49 | cp50 | cp51 | cp52 | cp53 | cp54 | cp55 | nc2 | cp57 | cp58 | cp59 | cp60 | cp61 | cp62 | cp63

dst-ip

Syntax **dst-ip** {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *prefix-list-name*}
no dst-ip

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

Description This command configures a destination IPv4 address range or specifies an IP prefix list configured under the **match-list ip-prefix-lis**t command to be used as a match criterion for an IP filter or IP exception filter.

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 can also be used.

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

Default n/a

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

Values 0.0.0.0 to 255.255.255.255

mask — the subnet mask length expressed as a decimal integer

Values 1 to 32

ipv4-address-mask — any mask expressed in dotted-decimal notation

Values 0.0.0.0 to 255.255.255.255

prefix-list-name — the name of the IP prefix list configured under the **match-list ip-prefix-list** command

dst-ip

Syntax **dst-ip** {*ipv6-address/prefix-length* | *ipv6-address ipv6-address-mask* | **ipv6-prefix-list** *prefix-list-name*}
no dst-ip

Context config>filter>ipv6-filter>entry>match

Description This command configures a destination IPv6 address range or specifies an IPv6 prefix list configured under the **match-list ipv6-prefix-list** command to be used as a match criterion for an IP filter.

To match on the destination IP address, specify the address and prefix length; for example, 11::12/128.

The **no** form of the command removes the destination IPv6 address or prefix list match criterion.

Default n/a

Parameters *ipv6-address* — the IPv6 address on the interface

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

prefix-length — the prefix length associated with the IPv6 address

Values 0 to 128

ipv6-address-mask — the IPv6 address mask

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

prefix-list-name — the name of the IPv6 prefix list configured with the **match-list ipv6-prefix-list** command

dst-mac

Syntax **dst-mac** *ieee-address*
no dst-mac

Context config>filter>mac-filter>entry>match

Description This command configures a destination MAC address to be used as a MAC filter match criterion.

To match on the destination MAC address, specify the IEEE address.

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

Default no dst-mac

Parameters *ieee-address* — the MAC address to be used as a match criterion

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where x is a hexadecimal digit

dst-port

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

Context config>filter>ip-exception>entry>match
config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

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

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

Default n/a

Parameters **lt | gt | eq** — use relative to *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 — specifies an inclusive range of port numbers to be used as a match criteria. The first *dst-port-number* specifies the start of the range, and the second *dst-port-number* specifies the end of the range.

etype

Syntax **etype** *0x600...0xffff*
no etype

Context config>filter>mac-filter>entry>match

Description This command configures an Ethernet type II Ethertype value to be used as a MAC filter match criterion.

The Ethernet type field is a 2-byte field used to identify the protocol carried by the Ethernet frame. For example, 0800 is used to identify IPv4 packets. The Ethernet type II frame Ethertype value to be used as a match criterion can be expressed as a hexadecimal (0x0600 to 0xFFFF) or a decimal (1536 to 65535) value.

The Ethernet type field is used by the Ethernet version-II frames.

The **no** form of the command removes the previously entered etype field as the match criteria.

Default no etype

fragment

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

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

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

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

This command applies to IPv4 filters only.

Default false

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

false — configures a match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.

icmp-code

Syntax **icmp-code** *icmp-code*
no icmp-code

Context config>filter>ip-exception>entry>match
config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures matching on the ICMP code field in the ICMP header of an IPv4 or IPv6 packet as a filter match criterion, or configures matching on the ICMP code field in the ICMP header of an IPv4 packet as an exception filter match criterion.

This command applies only 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* — *icmp-code-number* or *icmp-code-keyword*

icmp-code-number — the ICMP code number in decimal, hexadecimal, or binary, to be used as a match criterion

Values [0 to 250]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

icmp-code-keyword — the ICMP code keyword to be used as a match criterion

Values **For IPv6:**
none, no-route-to-destination, comm-with-dest-admin-prohibited, beyond-scope-src-addr, address-unreachable, port-unreachable
For IPv4 and IP-exception:
none, network-unreachable, host-unreachable, protocol-unreachable, port-unreachable, fragmentation-needed, source-route-failed, dest-network-unknown, dest-host-unknown, src-host-isolated, network-unreachable-for-tos, host-unreachable-for-tos

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context config>filter>ip-exception>entry>match
config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures matching on the ICMP type field in the ICMP header of an IPv4 or IPv6 packet as a filter match criterion, or configures matching on the ICMP type field in the ICMP header of an IPv4 packet as an exception filter match criterion.

This command applies only 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* — *icmp-type-number* or *icmp-type-keyword*

icmp-type-number — the ICMP type number in decimal, hexadecimal, or binary, to be used as a match criterion

Values [0 to 250]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

icmp-type-keyword — the ICMP type to be used as a match criterion

Values **For IPv6:**

none, dest-unreachable, packet-too-big, time-exceeded, parameter-problem, echo-request, echo-reply, multicast-listen-query, multicast-listen-report, multicast-listen-done, router-solicitation, router-advt, neighbor-solicitation, neighbor-advertisement, redirect-message, router-renumbering, icmp-node-info-query, icmp-node-info-resp, inv-nd-solicitation, inv-nd-adv-message, multicast-listener-report-v2, home-agent-ad-request, home-agent-ad-reply, mobile-prefix-solicitation, mobile-prefix-advt, cert-path-solicitation, cert-path-advt, multicast-router-advt, multicast-router-solicitation, multicast-router-termination, fmipv6, rpl-control, ilnpv6-locator-update, duplicate-addr-request, duplicate-addr-confirmation

For IPv4 and IP-exception:

none, echo-reply, dest-unreachable, source-quench, redirect, echo-request, router-advt, router-selection, time-exceeded, parameter-problem, timestamp-request, timestamp-reply, addr-mask-request, addr-mask-reply, photuris

ip-option

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

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

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

The option type octet contains three fields:

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

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

This command applies to IPv4 filters only.

Default no ip-option

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

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

Values 0 to 255

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

This 8-bit mask can be entered using decimal, hexadecimal, or binary formats (see Table 79).

Table 79 **8-bit mask formats**

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

Default 255 (decimal) (exact match)

Values 0 to 255

multiple-option

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

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

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

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

This command applies to IPv4 filters only.

Default no multiple-option

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

false — specifies matching on IP packets that do not contain multiple option fields in the header

option-present

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

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

Description This command configures matching packets that contain the option field or have an option field of 0 in the IP header as an IP filter match criterion.

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

This command applies to IPv4 filters only.

Parameters **true** — specifies matching on all IP packets that contain the option field in the header. A match will occur for all packets that have the option field present. An option field of 0 is considered as no option present.

false — specifies matching on IP packets that do not have any option field present in the IP header (an option field of 0)

src-ip

Syntax **src-ip** {*ip-address/mask* | *ip-address ipv4-address-mask* | **ip-prefix-list** *prefix-list-name*}
no src-ip

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

Description This command configures a source IPv4 address range or specifies an IP prefix list configured under the **match-list ip-prefix-list** command to be used as a match criterion for an IP filter or IP exception filter.

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 can also be used.

The **no** form of the command removes the source IP address or prefix list 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

ipv4-address-mask — any mask expressed in dotted-decimal notation

Values 0.0.0.0 to 255.255.255.255

prefix-list-name — the name of the IP prefix list configured with the **match-list ip-prefix-list** command

src-ip

Syntax **src-ip** {*ipv6-address/prefix-length* | *ipv6-address ipv6-address-mask* | **ipv6-prefix-list** *prefix-list-name*}
no src-ip

Context config>filter>ipv6-filter>entry>match

Description This command configures a source IPv6 address range or specifies an IPv6 prefix list configured under the **match-list ipv6-prefix-list** command to be used as a match criterion for an IP filter.

To match on the source IP address, specify the address and prefix length; for example, 11::12/128.

The **no** form of the command removes the source IPv6 address or prefix list match criterion.

Default n/a

Parameters *ipv6-address* — the IPv6 address on the interface

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

d: [0 to 255]D

prefix-length — the prefix length associated with the IPv6 address

Values 0 to 128

ipv6-address-mask — the IPv6 address mask

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

prefix-list-name — the name of the IPv6 prefix list configured with the **match-list ipv6-prefix-list** command

src-mac

Syntax **src-mac** *ieee-address*
no src-mac

Context config>filter>mac-filter>entry>match

Description This command configures a source MAC address to be used as a MAC filter match criterion.

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

Default no src-mac

Parameters *ieee-address* — the 48-bit IEEE MAC address to be used as a match criterion

Values xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where x is a hexadecimal digit

src-port

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

Context config>filter>ip-exception>entry>match
config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures a source TCP or UDP port number or port range for an IP filter or IP exception 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 — specifies an inclusive range of port numbers to be used as a match criteria. The first *src-port-number* specifies the start of the range, and the second *src-port-number* specifies the end of the range.

tcp-ack

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

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

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

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

Default no tcp-ack

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

false — specifies matching on IP packets that do not have the ACK bit set in the control bits of the TCP header of the IP packet

tcp-syn

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

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

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

The SYN bit is normally set when the source of the packet wants to initiate a TCP session with the specified destination IP address.

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

Default no tcp-syn

Parameters **true** — specifies matching on IP packets that have the SYN bit set in the control bits of the TCP header

false — specifies matching on IP packets that do not have the SYN bit set in the control bits of the TCP header

5.7.2.1.7 Security Policy Commands

abort

Syntax **abort**

Context config>security

Description This command discards changes made to a security feature.

Default n/a

begin

Syntax **begin**

Context config>security

Description This command enters the mode to create or edit security features.

Default n/a

commit

Syntax **commit**

Context config>security

Description This command saves changes made to security features.

Default n/a

app-group

Syntax **app-group** {*group-id* | *name*} [**create**]
no app-group {*group-id* | *name*}

Context config>security

Description This command enters the context for creating an application group to be used in a security policy.

The **no** form of the command removes the configured application group.

Default n/a

Parameters *group-id* — the application group ID, from 1 to 100

name — the name of the application group, up to 32 characters in length (must start with a letter)

name

Syntax **name** *name*
no name

Context config>security>app-group
config>security>host-group
config>security>policer-group

Description This command configures a name for an application group, host group, or policer group.

The **no** form of the command removes the configured name.

Parameters *name* — the name of the application group, host group, or policer group, up to 32 characters in length (must start with a letter)

bypass

Syntax **bypass** {*bypass-id* | *name*} [**create**]
no bypass {*bypass-id* | *name*}

Context config>security

Description This command creates a bypass policy that allows packets to bypass a firewall in a Layer 2 service security zone based on specified match criteria. The bypass policy must be given an ID or a name that is unique within the system. If given a name, the system automatically assigns the first available ID number to the policy. The bypass name can be used instead of the bypass ID to refer to a bypass policy for firewall configuration commands, show commands, monitor commands, clear commands, and service endpoint association commands. The bypass policy can be associated with a VPLS or Epipe service with the **fw-bypass-policy** command under the **config>service>vpls** or **config>service>epipe** context.

Each bypass policy that is created uses one of the system's filter entry slots.

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

Default n/a

Parameters *bypass-id* — the bypass ID number

Values 1 to 65535

name — the name of the bypass policy

Values 1 to 32 characters (must start with a letter). If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

create — keyword required when first creating the bypass policy. When the policy is created, you can enter the context without the **create** keyword.

entry

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

Context config>security>bypass

Description This command configures an entry in a bypass policy.

The **no** form of this command deletes the entry with the specified ID. When an entry is deleted, all configuration parameters for the entry are also deleted.

Default n/a

Parameters *entry-id* — the entry ID number

Values 1 to 65535

create — keyword required when first creating the entry. When the entry is created, you can enter the context without the **create** keyword.

match

Syntax **match** [**protocol** *protocol-id*]
no match

Context config>security>bypass>entry

Description This command defines the protocols that are allowed to bypass a firewall in a Layer 2 service.

When processing protocol packets defined in the bypass policy, the 7705 SAR ignores the firewall lookup table, even if there is a more specific matching rule for the firewall. The bypass policy must be created carefully to ensure that it does not cause any security holes on the node.

The **no** form of the command removes the protocol from the bypass policy.

Default no protocol

Parameters *protocol-id — protocol-number* | *protocol-name*

protocol-number — the protocol number in decimal, hexadecimal, or binary, that is allowed to bypass the firewall. See Table 80 for a list of common protocol numbers.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — the name of the protocol that is allowed to bypass the firewall

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip
* - udp/tcp wildcard

Table 80 **IP Protocol IDs and Descriptions**

Protocol ID	Protocol	Description
1	icmp	Internet Control Message
2	igmp	Internet Group Management
4	ip	IP in IP (encapsulation)
6	tcp	Transmission Control
8	egp	Exterior Gateway Protocol
9	igp	Any private interior gateway
17	udp	User Datagram
27	rdp	Reliable Data Protocol
41	ipv6	IPv6
43	ipv6-route	Routing Header for IPv6
44	ipv6-frag	Fragment Header for IPv6
45	idrp	Inter-Domain Routing Protocol
46	rsvp	Reservation Protocol
47	gre	General Routing Encapsulation
58	ipv6-icmp	ICMP for IPv6
59	ipv6-no-nxt	No Next Header for IPv6
60	ipv6-opts	Destination Options for IPv6
80	iso-ip	ISO Internet Protocol
88	eigrp	EIGRP

Table 80 **IP Protocol IDs and Descriptions (Continued)**

Protocol ID	Protocol	Description
89	ospf-igp	OSPFIGP
97	ether-ip	Ethernet-within-IP Encapsulation
98	encap	Encapsulation Header
102	pnni	PNNI over IP
103	pim	Protocol Independent Multicast
112	vrrp	Virtual Router Redundancy Protocol
115	l2tp	Layer Two Tunneling Protocol
118	stp	Schedule Transfer Protocol
123	ptp	Performance Transparency Protocol
124	isis	ISIS over IPv4
126	crtp	Combat Radio Transport Protocol
127	crudp	Combat Radio User Datagram
132	sctp	Stream Control Transmission Protocol
137	mpls-in-ip	MPLS in IP

dst-port

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

Context config>security>bypass>entry>match

Description This command configures a destination protocol TCP or UDP port number or port range for the bypass policy match criterion.

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

Default no dst-port

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

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

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

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

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

Values 1 to 65535

range — specifies an inclusive range of port numbers to be used as a match criterion. The first *dst-port-number* specifies the start of the range, and the second *dst-port-number* specifies the end of the range.

src-port

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

Context config>security>bypass>entry>match

Description This command configures a source protocol TCP or UDP port number or port range for the bypass policy 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 criterion:

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

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

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

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

Values 1 to 65535

range — specifies an inclusive range of port numbers to be used as a match criterion. The first *src-port-number* specifies the start of the range, and the second *src-port-number* specifies the end of the range.

name

Syntax **name** *name*
no name

Context config>security>bypass

Description This command configures the bypass policy name. The bypass policy name must be unique within the system. If the policy name was already configured with the bypass command, this command renames the policy.

The **no** form of the command deletes the bypass name.

Default no name

Parameters *name* — the name of the bypass policy

Values 1 to 32 characters (must start with a letter). If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

host-group

Syntax **host-group** {*group-id* | *name*} [**create**]
no host-group {*group-id* | *name*}

Context config>security

Description This command enters the context for creating a host group to be used in a security policy.

The **no** form of the command removes the configured host group.

Default n/a

Parameters *group-id* — the host group ID, from 1 to 100

name — the name of the host group, up to 32 characters in length (must start with a letter)

host

Syntax **host** *ip-address* [**to** *ip-address*]
no host

Context config>security>host-group

Description This command configures a range of hosts to be used in a host group. Up to 10 entries can be configured for a host group.

Default n/a

Parameters *ip-address* — the IPv4 address of the host

logging

Syntax **logging**

Context config>security

Description This command enters the security logging context.

Default n/a

log-id

Syntax **log-id** {*log-id* | *log-name*} [**create**]
no log-id {*log-id* | *log-name*}

Context config>security>logging

Description This command configures the identifier for the security log. The 7705 SAR supports up to 100 security logs. This log ID can be applied at the zone level or at the rule level, but not to both at the same time.

The **no** form of the command removes the configured security group.

Default n/a

Parameters *log-id* — the security log ID, from 1 to 100

log-name — the name of the security log, up to 32 characters in length (must start with a letter)

destination

Syntax **destination** {**memory** [*size*] | **syslog** *syslog-id*}
no destination

Context config>security>logging>log

Description This command configures the destination location of the specified security log.

Default n/a

Parameters **memory** — specifies that the log destination is the 7705 SAR local memory (compact flash or flash drive)

size — the number of log events that can be held in memory, up to 1024

syslog — specifies that the log destination is the system log

syslog-id — the identifier of the system log, up to 32 characters in length

name

Syntax **name** *name*
no name

Context config>security>logging>log

Description This command configures the name of the specified security log.

Default n/a

Parameters *name* — the name of the security log, up to 32 characters in length

profile

Syntax **profile** {*logging-profile-id* | *logging-profile-name*}

Context config>security>logging>log

Description This command configures the logging profile to which the specified security log will match events.

Default n/a

Parameters *logging-profile-id* — the logging profile ID for the security log

Values 1 to 100

logging-profile-name — the logging profile name for the security log, up to 32 characters in length

shutdown

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

Context config>security>logging>log

Description This command disables logging to the specified security log. Logging is enabled by default.

The **no** form of this command enables logging to the specified security profile.

Default no shutdown

wrap-around

Syntax [**no**] **wrap-around**

Context config>security>logging>log

Description This command enables log wraparound when the maximum log size has been reached in the log destination location. When wraparound is enabled, the log starts over at 1 and overwrites the existing logs when the log size is at maximum. When wraparound is disabled, the log stops adding entries when the log size is at maximum.

The **no** form of this command disables log wraparound.

Default no wrap-around

profile

Syntax **profile** {*profile-id* | *profile-name*} [**create**]
no profile {*profile-id* | *profile-name*}

Context config>security>logging

Description This command configures the security logging profile.

The **no** form of the command removes the configured profile.

Default n/a

Parameters *profile-id* — the ID of the profile group, from 1 to 65535

profile-name — the name of the profile group, up to 32 characters in length

event-control

Syntax **event-control** *event-type* [**event** *event*] {**suppress** | **throttle** | **off**}

Context config>security>logging>profile

Description This command controls the generation of security log events. A log can be configured to generate all event types and events, or to generate specific event types and events. In addition, for each event type or event, one of three actions can be configured: suppress, throttle, or off. These configurations all become part of the specified logging profile. Table 81 lists the supported event types and events on 7705 SAR firewalls.

Table 81 **Event Types and Events Supported on 7705 SAR Firewalls**

Event Type	Event
Packet	TcpInvalidHeader DnsInvalidHeader DnsUnmatchedAnswer IcmpUnmatchedReply TcpInvalidFlagCombination TcpRst PolicyErrorFrag FragDropAction DuplicateFrag LandAttack
Zone	NoRuleMatched SessionLimitReached
Policy	Matched MatchedNAT ActionReject MaxConcurrentUsesReached FragsNotAccepted TcpSynReqdtoEstablish
Session	SessionBegin SessionEnd SessionBeginEnd RuleActionDrop ProhibitedIpOption InvalidIcmpT3 PktLimitReached

Table 81 **Event Types and Events Supported on 7705 SAR Firewalls (Continued)**

Event Type	Event
Application	Summary HandshakeMissing HandshakeCtlInvalid HandshakeDataUnexpected OptError OptBadLen OptTTcpForbidden OptNonStdForbidden OptTStampMissing OptTStampUnexpected TStampTooOld TStampEchoInvalid ScaleUnexpected SeqNumOutside AckNumOutside AckNumNotZero AckNumStale AckUnexpected AckMissing FlagsSynRst SynUnexpected SynMissing FinUnexpected InvCksum ConnReused RstSeqNumUnexpected TTL NotFullHeader FlagsSynFin SplitHandshake

Table 81 **Event Types and Events Supported on 7705 SAR Firewalls (Continued)**

Event Type	Event
ALG	CmdIncomplete DynamicRuleInserted DynamicRuleInsertedPASV CannotInsertDynamicRule CannotInsertDynamicRulePASV BadCmdSyntax BadPortCmdSyntax BadPasvCmdSyntax BadAddrSyntax TftpDynRuleInsertErr TftpDynRuleInserted

Default n/a

Parameters *event-type* — the type of event to be controlled for in this logging profile, as shown in Table 81

event — the name of the event to be controlled for in this logging profile as shown in Table 81

suppress — suppresses the specified event type or event in this logging profile

throttle — throttles a repeating event type or event when the same event type or event is generated repeatedly within 1 s in this logging profile

off — allows the event type or event to be logged in this logging profile

name

Syntax **name** *name*
no name

Context config>security>logging>profile

Description This command configures a name for this logging profile.

The **no** form of the command removes the configured name for this logging profile.

Default n/a

Parameters *name* — the name of the logging profile, up to 32 characters in length

profile

Syntax **profile** {*profile-id* | *profile-name*} [**create**]
no profile {*profile-id* | *profile-name*}

Context config>security

Description This command configures a profile group that provides a context within which you can configure security features such as session idle timeouts and application assurance parameters. Profile 1 is a default profile and cannot be modified.

The **no** form of the command removes the configured profile group.

Default 1

Parameters *profile-id* — the ID of the profile group, from 1 to 100

profile-name — the name of the profile group, up to 32 characters in length

application

Syntax **application**

Context config>security>profile

Description This command enters the application context for firewall configuration.

alg

Syntax **alg** {**auto** | **ftp** | **tftp**}
no alg

Context config>security>profile>app

Description This command enables application level gateway (ALG) inspection by the firewall.

The **no** form of the command disables ALG inspection by the firewall.

Default n/a

Parameters **auto** — specifies that the firewall automatically determines the application traffic that requires inspection

ftp — specifies that the firewall must inspect FTP application traffic as determined by the port matching criteria in the security policy and apply the FTP ALG to the command traffic. This option should be used when FTP ALG is required on any TCP port being used for FTP.

tftp — specifies that the firewall must inspect TFTP application traffic as determined by the port matching criteria in the security policy and apply the TFTP ALG to the command traffic. This option should be used when TFTP ALG is required on any UDP port being used for TFTP.

assurance

Syntax [**no**] **assurance**

Context config>security>profile>app

Description This command enables the context for configuring application assurance parameters. Enabling application assurance automatically sets the defaults for the parameters as listed in Table 82.

Table 82 **Application Assurance Parameter Default Values**

Parameter	Default Value
DNS	reply-only
ICMP	limit-type3
IP	options permit-any
TCP	no strict

The **no** form of the command disables application assurance on the firewall.

Default n/a

dns

Syntax **dns**

Context config>security>profile>aa

Description This command enables the context for configuring DNS inspection parameters on a firewall in the application assurance parameters context.

Default n/a

reply-only

Syntax [**no**] **reply-only**

Context config>security>profile>aa>dns

Description This command limits the number of replies to DNS requests. When enabled, the firewall permits a single reply to each DNS request.

The **no** form of the command disables the limiting of DNS replies; the firewall permits all replies to each DNS request.

Default reply-only

icmp

Syntax **icmp**

Context config>security>profile>aa

Description This command enables the context for configuring ICMP limit parameters on a firewall in the application assurance parameters context.

Default n/a

limit-type3

Syntax [**no**] **limit-type3**

Context config>security>profile>aa>icmp

Description This command limits the number of ICMP type 3 replies through a firewall. When enabled, only 15 ICMP type 3 replies are permitted through the firewall for each ICMP and IP session.

The **no** form of the command disables the limiting of ICMP type 3 replies through a firewall; all ICMP type 3 replies are permitted through the firewall for each ICMP and IP session.

Default limit-type3

request-limit

Syntax **request-limit** *packets*
no request-limit

Context config>security>profile>aa>icmp

Description This command configures the number of ICMP requests and replies allowed through the firewall for each ICMP session. Any requests or replies that are received beyond the configured limit are discarded until the ICMP session times out.

The **no** form of the command allows all ICMP requests and replies through the firewall for each ICMP session.

Default 5

Parameters *packets* — the maximum number of ICMP request and reply packets permitted through the firewall for each ICMP session, from 1 to 15

ip

Syntax **ip**

Context config>security>profile>aa

Description This command enables the context for configuring IP layer inspection on a firewall in the application assurance parameters context.

Default n/a

options

Syntax **options** {**permit** *ip-option-mask* | **permit-any**}
options *ip-option-name* [*ip-option-name*]

Context config>security>profile>aa>ip

Description This command controls the inspection of IP options in an IP packet header. The IP options can be specified using either the bit mask value or the name.

The **permit** command only applies when using bit mask values. It allows packets through the firewall when the IP options on those packets match the bit mask value specified in the *ip-option-mask* parameter. The *ip-option-mask* is a flat bit representation of the IP Option Number. The IP Option Copy Bit and IP Option Class Bits are omitted from the *ip-option-mask*. For example, to permit a packet with the router alert option (which uses IP Option Number 20), bit 20 of the *ip-option-mask* should be set, which configures the *ip-option-mask* parameter as 0x00100000. To discard all IP packets with IP options, configure the *ip-option-mask* parameter as 0x0. To permit any option, configure the *ip-option-mask* parameter as 0xffffffff or use the **permit-any** command. When **permit-any** is configured, the 7705 SAR does not examine IP options and allows all packets through the firewall.

Multiple options can be permitted in a single line of configuration by “AND”ing the IP option bit mask values. For example, to permit packets with the router alert, EOOL, and NOP options, configure the *ip-option-mask* parameter as 0x00100003.

When IP options are specified using *ip-option-name*, the **permit** command is implied. Multiple options can be specified by listing multiple names.

Table 83 lists the names and bit mask values of the supported IP options.

Table 83 **Supported IP Options**

IP Option Number	IP Option Value	IP Option Name	Bit Mask Value
0	0	EOOL – End of Options List	0x00000001
1	1	NOP – No Operation	0x00000002
2	130	SEC – Security	0x00000004
3	131	LSR – Loose Source Route	0x00000008
4	68	TS – time Stamp	0x00000010
5	133	E-SEC – Extended Security	0x00000020
6	134	CIPSO – Commercial Security	0x00000040
7	7	RR – Record Route	0x00000080
8	136	SID – Stream ID	0x00000100
9	137	SSR – Strict Source Route	0x00000200
10	10	ZSU – Experimental Measurement	0x00000400
11	11	MTUP – MTU Probe	0x00000800
12	12	MTUR – MTU Reply	0x00001000
13	205	FINN – Experimental Flow Control	0x00002000
14	142	VISA – Experimental Access Control	0x00004000
15	15	Encode	0x00008000
16	144	IMITD – IMI Traffic Descriptor	0x00010000
17	145	EIP – Extended Internet Protocol	0x00020000
18	82	TR – Traceroute	0x00040000
19	147	ADDEXT – Address Extension	0x00080000
20	148	RTRALT – Router Alert	0x00100000
21	149	SDB – Selective Directed Broadcast	0x00200000

Table 83 **Supported IP Options (Continued)**

IP Option Number	IP Option Value	IP Option Name	Bit Mask Value
22	150	unassigned	0x00400000
23	151	DPS – Dynamic Packet State	0x00800000
24	152	UMP – Upstream Multicast Packet	0x01000000
25	25	QS – Quick-Start	0x02000000
30	30	EXP – RFC3692-style experiment	0x40000000
30	94	EXP – RFC3692-style experiment	0x40000000
30	158	EXP – RFC3692-style experiment	0x40000000
30	222	EXP – RFC3692-style experiment	0x40000000

Default permit-any

Parameters **permit** — allows packets with the specified IP options through the firewall

ip-option-mask — the IP options to be matched by the firewall, up to 11 characters (in decimal, hexadecimal, or binary)

ip-option-name — the IP option name to be matched by the firewall; up to 30 option names can be specified

Values nop | sec | lsr | ts |e-sec | cipso | rr | sid | ssr | zsu | mtup | mtur | finn | visa | encode | imitd | eip | tr | addext | rtralt | sdb | 15 | dps | ump | qs | 26 | 27 | 28 | 29 | exp

permit-any — allows packets with any IP options through the firewall

tcp

Syntax **tcp**

Context config>security>profile>aa

Description This command enables the context for configuring TCP layer inspection on a firewall in the application assurance parameters context.

Default n/a

strict

Syntax [**no**] **strict**

Context config>security>profile>aa>tcp

Description This command enables strict examination of TCP packets through the firewall. When enabled, the firewall examines the header of each TCP packet for that session to ensure compliance with RFC 793.

Note: The TCP sessions that are configured with strict TCP are processed in the 7705 SAR CSM complex. Aggregate throughput of sessions through the CSM is limited by the processing power of the CSM that is performing multiple tasks. Throughput for a session on the CSM will not match the maximum throughput of a session that only traverses the datapath.

The **no** form of the command disables examination of the TCP header on each TCP packet.

Default no strict

fwd-policer-group

Syntax **fwd-policer-group** {*group-id* | *name*}
no fwd-policer-group

Context config>security>profile

Description This command configures a forward policer group for a security profile. A TCP/UDP security session is bidirectional. When a security sessions is created from a private domain to a public domain, the session's forward direction is from the private to the public domain and the session's reverse direction is from the public to the private domain. A forward-direction policer group acts on traffic that is traversing from the private domain to the public domain.

The **no** form of the command removes the configured forward policer group.

Parameters *group-id* — the identifier of the forward policer group associated with this security profile, from 1 to 1024

name — the name of the forward policer group associated with this security profile, up to 32 characters in length (must start with a letter)

name

Syntax [**no**] **name** *profile-name*

Context config>security>profile

Description This command configures a profile group name.

The **no** form of the command removes the configured profile group name.

Parameters *profile-name* — the name of the profile, up to 32 characters in length (must start with a letter)

rev-policer-group

Syntax **rev-policer-group** {*group-id* | *name*}
no rev-policer-group

Context config>security>profile

Description This command configures a reverse policer group for a security profile. A TCP/UDP security session is bidirectional. When a security sessions is created from a private domain to a public domain, the session's forward direction is from the private to the public domain and the session's reverse direction is from the public to the private domain. A reverse-direction policer group acts on traffic that is traversing from the public domain to the private domain.

The **no** form of the command removes the configured reverse policer group.

Parameters *group-id* — the identifier of the reverse policer group associated with this security profile, from 1 to 1024

name — the name of the reverse policer group associated with this security profile, up to 32 characters in length (must start with a letter)

timeouts

Syntax **timeouts**

Context config>security>profile

Description This command configures session idle timeouts for this profile.

icmp-request

Syntax **icmp-request** [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
no icmp-request

Context config>security>profile>timeouts

Description This command sets the timeout for an ICMP security session. An ICMP session is based on the packet source and destination IP addresses and ICMP identifier. This timer removes the ICMP session if no ICMP packets have been received for the configured time.

The **no** form of the command removes the timeout set for **icmp-request**.

Default 60 s

Parameters *minutes* — the timeout in minutes

Values 1 to 4

seconds — the timeout in seconds

Values 1 to 59

other-sessions

Syntax **other-sessions** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
no other-sessions

Context config>security>profile>timeouts

Description This command sets the timeout for protocol sessions other than TCP, UDP, or ICMP. These other protocol sessions are based on a 3-tuple match of source IP address, destination IP address, and protocol, except for SCTP (protocol 132), which uses a 5-tuple match like UDP. If no packets are received after the configured time, the firewall session is discontinued and removed from the 7705 SAR.

The **no** form of the command removes the timeout set for **other-sessions**.

Default n/a

Parameters *days* — the timeout in days

Values 1

hours — the timeout in hours

Values 1 to 23

minutes — the timeout in minutes

Values 1 to 59

seconds — the timeout in seconds

Values 1 to 59

strict — configures the timer to time out after the last session transition state

idle — configures the timer to time out when no packets have arrived on the session for the configured period

tcp-established

Syntax **tcp-established** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
no tcp-established

Context config>security>profile>timeouts

Description This command sets the timeout for a TCP session in the established state.

The **no** form of the command removes the timeout set for **tcp-established**.

Default n/a

Parameters *days* — the timeout in days

Values 1

hours — the timeout in hours

Values 1 to 24

minutes — the timeout in minutes

Values 1 to 59

seconds — the timeout in seconds

Values 1 to 59

tcp-syn

Syntax **tcp-syn** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no tcp-syn

Context config>security>profile>timeouts

Description This command configures the timeout applied to a TCP session in the SYN state.

The **no** form of the command removes the timeout set for **tcp-syn**.

Default n/a

Parameters *days* — the timeout in days

Values 1

hours — the timeout in hours

Values 1 to 24

minutes — the timeout in minutes

Values 1 to 59

seconds — the timeout in seconds

Values 1 to 59

tcp-time-wait

Syntax **tcp-time-wait** [**min** *minutes*] [**sec** *seconds*]
no tcp-time-wait

Context config>security>profile>timeouts

Description This command configures the timeout applied to a TCP session in a time-wait state.

The **no** form of the command removes the timeout set for **tcp-time-wait**.

Default n/a

Parameters *minutes* — the timeout in minutes

Values 1 to 4

seconds — the timeout in seconds

Values 1 to 59

tcp-transitory

Syntax **tcp-transitory** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*]
no tcp-transitory

Context config>security>profile>timeouts

Description This command configures the idle timeout applied to a TCP session in a transitory state.

The **no** form of the command removes the timeout set for **tcp-transitory**.

Default n/a

Parameters *days* — the timeout in days

Values 1

hours — the timeout in hours

Values 1 to 24

minutes — the timeout in minutes

Values 1 to 59

seconds — the timeout in seconds

Values 1 to 59

udp

Syntax **udp** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
no udp

Context config>security>profile>timeouts

Description This command configures the UDP mapping timeout.

The **no** form of the command removes the UDP mapping timeout.

Default n/a

Parameters *days* — the timeout in days

Values 1

hours — the timeout in hours

Values 1 to 24

minutes — the timeout in minutes

Values 1 to 59

seconds — the timeout in seconds

Values 1 to 59

udp-dns

Syntax **udp-dns** [**days** *days*] [**hrs** *hours*] [**min** *minutes*] [**sec** *seconds*] [**strict** | **idle**]
no udp-dns

Context config>security>profile>timeouts

Description This command configures the timeout applied to a UDP session with destination port 53.

The **no** form of the command removes the **udp-dns** timeout.

Default n/a

Parameters *days* — the timeout in days

Values 1

hours — the timeout in hours

Values 1 to 24

minutes — the timeout in minutes

Values 1 to 59

seconds — the timeout in seconds

Values 1 to 59

udp-initial

Syntax **udp-initial** [**min** *minutes*] [**sec** *seconds*]
no udp-initial

Context config>security>profile>timeouts

Description This command configures the timeout applied to a UDP session in its initial state.

The **no** form of the command removes the **udp-initial** timeout.

Default n/a

Parameters *minutes* — the timeout in minutes

Values 1 to 5

seconds — the timeout in seconds

Values 1 to 59

policer-group

Syntax **policer-group** {*group-id* | *name*} [**create**]
no policer-group {*group-id* | *name*}

Context config>security

Description This command enters the context for creating a policer group to be used in a security profile.

The **no** form of the command removes the configured policer group.

Parameters *group-id* — the ID of the policer group, from 1 to 1024

name — the name of the policer group, up to 32 characters in length (must start with a letter)

rate

Syntax **rate** *rate* **cbs** *size* [**bytes** | **kilobytes**]
no rate

Context config>security>policer-group

Description This command sets the policer rate and CBS buffer size for the policer group.

Parameters *rate* — the policer rate, in Mb/s

Values 1 to 10000

size — the CBS buffer size, in bytes

Values 1 to 130816

policy

Syntax **policy** {*policy-id* | *policy-name*} [**create**]
no policy {*policy-id* | *policy-name*}

Context config>security

Description This command configures a policy group that provides a context within which you can configure a security policy.

The **no** form of the command removes the configured policy group.

Default n/a

Parameters *policy-id* — the ID of the policy group, from 1 to 65535

policy-name — the name of the policy group, up to 32 characters in length

entry

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

Context config>security>app-group
config>security>policy

Description This command configures an entry in a security policy or in an application group.

The **no** form of this command deletes the entry with the specified ID. When an entry is deleted, all configuration parameters for the entry are also deleted.

Parameters *entry-id* — the entry ID number

Values 1 to 65535 for a security policy
1 to 65535 for an application group

action

Syntax **action** {**forward** | **reject** | **drop** | **nat**}

Context config>security>policy>entry

Description This command specifies what action to take (forward, reject, drop, or NAT) when packets match the entry criteria. An action must be specified in order for the entry to be active. If no action is specified, the entry is inactive.

The **nat** and **forward** actions each cause a 6-tuple lookup (source/destination IP address, source/destination port number, protocol, and source zone).

The **drop** action configures a firewall session on the datapath with the action to drop packets that match the entry criteria. The **drop** action should be used when an IP connection is carrying a large amount of traffic and CSM processing resources need to be preserved, because the **drop** action means that packets will not be extracted to the CSM to be rejected. Drop sessions are unidirectional and can be used as a way of blocking traffic from a source issuing a denial of service (DoS) attack.

Entering multiple action statements will overwrite previous action statements.

The **no** form of the command removes the specified **action** statement.

Default no action

Parameters **reject** — specifies that packets matching the entry criteria will be rejected on the CSM and no firewall session is created on the datapath

forward — specifies that packets matching the entry criteria will be forwarded and a firewall session is created on the datapath

drop — specifies that a firewall session is created on the datapath with the action to drop packets that match the entry criteria

nat — specifies that packets matching the entry criteria will have NAT applied to them and a NAT session is created on the datapath

action nat

Syntax **action nat** [**destination** *ip-address* **port** *tcp-udp-port*]

Context config>security>policy>entry

Description This command specifies the destination IP address and port to which packets that have NAT applied to them are sent.

NAT actions cause a 6-tuple lookup (source/destination IP address, source/destination port number, protocol, and source zone). If there is a match, NAT is applied and the packet is routed based on the datapath session table.

Entering multiple action statements will overwrite previous action statements.

The **no** form of the command removes the specified **action** statement. An entry is considered incomplete and is rendered inactive if no action is specified.

Default no action

Parameters *ip-address* — the static NAT (port forwarding) inside destination IP address to be used for port forwarding. When configured, the original packet destination IP address is overwritten with this IP address. This parameter applies only to static destination NAT (port forwarding).

Values 1.0.0.0 to 223.255.255.255

tcp-udp-port — the static NAT inside port IP number used for port forwarding. When configured, the original packet destination port number is overwritten with this port number. This parameter applies only to static destination NAT (port forwarding).

Values 1 to 65535

limit

Syntax [**no**] **limit**

Context config>security>policy>entry

Description This command is used to enter the limit context.

Default n/a

concurrent-sessions

Syntax **concurrent-sessions** *number*
no concurrent-sessions

Context config>security>policy>entry>limit

Description This command specifies the maximum number of concurrent security sessions that can be created for the specified policy.

The **no** form of the command returns the system to the default.

Default no concurrent-sessions

Parameters *number* — the number of concurrent sessions that can be programmed for the policy

Values 1 to 16383

fwd-direction-only

Syntax [**no**] **fwd-direction-only**

Context config>security>policy>entry>limit

Description This command forces a firewall to create a unidirectional session when a packet matches the criteria of the policy entry. In normal operating mode, when a packet matches the criteria and the packet is allowed through, the firewall creates a bidirectional session so that packets traveling in the reverse direction on that session are also allowed through the firewall.

The **no** form of the command creates a bidirectional firewall session for a matched packet.

Default no fwd-direction-only

logging

Syntax **logging** {**to log-id** {*log-id* | *name*} | **suppressed** | **to zone**}
no logging

Context config>security>policy>entry

Description This command configures logging control for this security policy entry. Logging can be enabled per entry using the **to log-id** command, or per zone using the **to zone** command. Logging is suppressed by default.

Default suppressed

Parameters **to log-id** — specifies to log events per entry

log-id — the log ID

Values 1 to 100

name — the log name, up to 32 characters in length

suppressed — specifies to suppress all logs generated by the entry

to zone — specifies to use the zone log settings

match

Syntax **match** [**protocol** *protocol-id*]
no match

Context config>security>app-group>entry

Description This command configures match criteria for an application group entry based on the specified protocol. An application group must be configured with at least one matching protocol before it can be assigned to a security policy.

When an application group is applied to NAT, the only protocols supported as match criteria are TCP, UDP, and ICMP.

The **no** form of the command removes the match criteria for the entry.

Default no match

Parameters *protocol-id — protocol-number | protocol-name*

protocol-number — the protocol number in decimal, hexadecimal, or binary, to be used as a match criterion. See Table 78 for a list of common protocol numbers.

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

protocol-name — the name of a protocol to be used as a match criterion. The 7705 SAR supports the protocols listed below.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip

match

Syntax **match** [**local**] [**protocol** *protocol-id*]
match [**app-group** {*group-id* | *name*}]
no match

Context config>security>policy>entry

Description This command configures match criteria for an entry based on the specified protocol or application group.

When a security policy is applied to NAT, the only protocols supported as match criteria are TCP, UDP, ICMP, and *.

The **no** form of the command removes the match criteria for the entry.

Default n/a

Parameters **local** — specifies that the destination IP address must be a local interface. The **local** parameter applies only to static destination NAT (port forwarding).

protocol-id — protocol-number | protocol-name

protocol-number — the protocol number in decimal, hexadecimal, or binary, to be used as a match criterion. See Table 78 for a list of common protocol numbers.

Values [0 to 255]D
[0x0 to 0xFF]H

[0b0 to 0b11111111]B

protocol-name — the name of a protocol to be used as a match criterion. The 7705 SAR supports the protocols listed below.

Values none, icmp, igmp, ip, tcp, egp, igp, udp, rdp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, ipv6-icmp, ipv6-no-nxt, ipv6-opts, iso-ip, eigrp, ospf-igp, ether-ip, encap, pnni, pim, vrrp, l2tp, stp, ptp, isis, crtp, crudp, sctp, mpls-in-ip, * — tcp/udp wildcard

group-id — the application group ID, from 1 to 100

name — the name of the application group, up to 32 characters in length (must start with a letter)

direction

Syntax **direction** {**zone-outbound** | **zone-inbound** | **both**}

Context config>security>policy>entry>match

Description This command sets the direction of the traffic to be matched against the IP criteria. For example, if **zone-inbound** is configured, then all inbound traffic to the zone has the match criteria applied to it.

Default both

Parameters **zone-outbound** — specifies packets that are outbound from the zone

zone-inbound — specifies packets that are inbound to the zone

both — specifies packets that are inbound to and outbound from the zone

dst-ip

Syntax **dst-ip** *ip-address* **to** *ip-address*
dst-ip host-group {*group-id* | *name*}
no dst-ip

Context config>security>policy>entry>match

Description This command configures the destination IP address or address range to be used in the matching criteria of a policy entry. All packets within the specified IP address range are processed for matching criteria. For host group matching criteria, the host group must be configured before adding it to the policy.

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

Default n/a

Parameters *ip-address* — the IPv4 address or address range to be matched

Values 0.0.0.1 to 255.255.255.255

group-id — the identifier of the host group to be matched

Values 1 to 100

name — the name of the host group to be matched, up to 32 characters in length (must start with a letter)

dst-port

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

Context config>security>policy>entry>match
config>security>app-group>entry>match

Description This command configures a destination protocol TCP or UDP port number or port range for the match criterion.

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

Default no dst-port

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

lt specifies that all port numbers less than the *port* number match

gt specifies that all port numbers greater than the *port* number match

eq specifies that the *port* number must be an exact match

port — the destination port number to be used as a match criterion, expressed as a decimal integer

Values 1 to 65535

start end — specifies an inclusive range of port numbers to be used as a match criterion. 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>security>policy>entry>match
config>security>app-group>entry>match

Description This command configures matching on an ICMP code field in the ICMP header of an IPv4 packet as a match criterion.

This option is only meaningful if the protocol match criterion specifies ICMP (1).

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

Default no icmp-code

Parameters *icmp-code — icmp-code-number* | *icmp-code-keyword*

icmp-code-number — the ICMP code number in decimal, hexadecimal, or binary, to be used as a match criterion

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

icmp-code-keyword — the name of an ICMP code to be used as a match criterion

Values none, network-unreachable, host-unreachable, protocol-unreachable, port-unreachable, fragmentation-needed, source-route-failed, dest-network-unknown, dest-host-unknown, src-host-isolated, network-unreachable-for-tos, host-unreachable-for-tos

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context config>security>policy>entry>match
config>security>app-group>entry>match

Description This command configures matching on the ICMP type field in the ICMP header of an IPv4 packet as a match criterion.

This option is only meaningful if the protocol match criterion specifies ICMP (1).

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

Default no icmp-type

Parameters *icmp-type — icmp-type-number* | *icmp-type-keyword*

icmp-type-number — the ICMP type number in decimal, hexadecimal, or binary, to be used as a match criterion

Values [0 to 255]D
[0x0 to 0xFF]H
[0b0 to 0b11111111]B

icmp-type-keyword — the name of an ICMP type to be used as a match criterion

Values none, echo-reply, dest-unreachable, source-quench, redirect, echo-request, router-advt, router-selection, time-exceeded, parameter-problem, timestamp-request, timestamp-reply, addr-mask-request, addr-mask-reply, photuris

src-ip

Syntax **src-ip** *ip-address* **to** *ip-address*
src-ip host-group {*group-id* | *name*}
no src-ip

Context config>security>policy>entry>match

Description This command configures the source IP address or address range to be used in the matching criteria of a policy entry. All packets within the specified IP address range are processed for matching criteria. For host group matching criteria, the host group must be configured before adding it to the policy.

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

Default n/a

Parameters *ip-address* — the IPv4 address to be matched

Values 0.0.0.1 to 255.255.255.255

group-id — the identifier of the host group to be matched

Values 1 to 100

name — the name of the host group to be matched, up to 32 characters in length (must start with a letter)

src-port

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

Context config>security>policy>entry>match
config>security>app-group>entry>match

Description This command configures a source protocol TCP or UDP port number or port range for the 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 *port* for specifying the port number match criterion:

lt specifies that all port numbers less than the *port* number match

gt specifies all port numbers greater than the *port* number match

eq specifies that the *port* number must be an exact match

port — the source port number to be used as a match criterion, expressed as a decimal integer

Values 1 to 65535

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

Values 1 to 65535

profile

Syntax **profile** {*profile-id* | *profile-name*}
no profile

Context config>security>policy>entry

Description This command assigns an already configured profile to a policy.

The **no** form of the command removes the assigned profile.

Default 1

Parameters *profile-id* — the ID of the profile group, from 1 to 65535

profile-name — the name of the profile group, up to 32 characters in length (must start with a letter)

name

Syntax **name** *policy-name*
no name

Context config>security>policy

Description This command configures a policy group name.

The **no** form of the command removes the configured policy group name.

Parameters *policy-name* — the name of the policy, up to 32 characters in length (must start with a letter)

session-high-wmark

Syntax **session-high-wmark** *percentage*
no session-high-wmark

Context config>security

Description This command configures the high-water mark threshold for security sessions. An alarm is raised when the high-water mark threshold is reached or exceeded. The value must be greater than or equal to the **session-low-wmark** value.

The **no** form of the command removes the high-water mark setting.

Default no session-high-wmark

Parameters *percentage* — specifies the high-water mark threshold

Values 1 to 100

session-low-wmark

Syntax **session-low-wmark** *percentage*
no session-low-wmark

Context config>security

Description This command configures the low-water mark threshold for security sessions. The alarm is cleared when the session utilization percentage is equal to or less than the low-water mark threshold. The value must be less than or equal to the **session-high-wmark** value.

The **no** form of the command removes the low-water mark setting.

Default no session-low-wmark

Parameters *percentage* — specifies the low-water mark threshold

Values 1 to 100

5.7.2.1.8 Match List Configuration Commands

match-list

Syntax **match-list**

Context config>filter

Description This command enables the context to configure a match list for use in IPv4, IPv6, IP exception, CSM, or management access filter policies.

Default n/a

ip-prefix-list

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

Context config>filter>match-list

Description This command creates an IPv4 prefix list that can be used as match criteria in filter policies.

An **ip-prefix-list** must contain only IPv4 address prefixes.

The **no** form of this command deletes the specified list. The list cannot be deleted if it is referenced by a filter policy.

Default n/a

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

create — keyword, mandatory when creating an **ip-prefix-list**

prefix

Syntax [**no**] **prefix** *ip-prefix/prefix-length*

Context config>filter>match-list>ip-prefix-list

Description This command adds an IPv4 prefix to the IPv4 address prefix match list.

To add a set of unique prefixes, execute the command with all unique prefixes. The prefixes are allowed to overlap IPv4 address space.

An IPv4 prefix addition will be blocked if resource exhaustion is detected anywhere in the system due to filter policies using this IPv4 address prefix list.

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

Default n/a

Parameters *ip-prefix/prefix-length* — a valid IPv4 address in dotted-decimal notation

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

prefix-exclude

Syntax [**no**] **prefix-exclude** *ip-prefix/prefix-length*

Context config>filter>match-list>ip-prefix-list

Description This command excludes an IPv4 prefix from the IPv4 address prefix match list.

The **no** form of this command deletes the specified excluded IPv4 prefix from the list.

Default n/a

Parameters *ip-prefix/prefix-length* — a valid IPv4 address in dotted-decimal notation

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

ipv6-prefix-list

Syntax **ipv6-prefix-list** *ipv6-prefix-list-name* [**create**]
no ipv6-prefix-list *ipv6-prefix-list-name*

Context config>filter>match-list

Description This command creates an IPv6 prefix list that can be used as match criteria in filter policies.

An **ipv6-prefix-list** must contain only IPv6 address prefixes.

The **no** form of this command deletes the specified list. The list cannot be deleted if it is referenced by a filter policy.

Default n/a

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

create — keyword, mandatory when creating an **ipv6-prefix-list**

prefix

Syntax [**no**] **prefix** *ipv6-prefix/prefix-length*

Context config>filter>match-list>ipv6-prefix-list

Description This command adds an IPv6 address prefix to the IPv6 address prefix match list.

To add a set of unique prefixes, execute the command with all unique prefixes. The prefixes are allowed to overlap IPv6 address space.

An IPv6 prefix addition will be blocked if resource exhaustion is detected anywhere in the system due to filter policies using this address prefix list.

The **no** form of this command deletes the specified IPv6 address prefix from the list.

Default n/a

Parameters *ipv6-prefix/prefix-length* — a valid IPv6 address prefix

Values *ipv6-prefix* — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D
prefix-length — 1 to 128

prefix-exclude

Syntax [**no**] **prefix-exclude** *ipv6-prefix/prefix-length*

Context config>filter>match-list>ipv6-prefix-list

Description This command excludes an IPv6 prefix from the IPv6 address prefix match list.

The **no** form of this command deletes the specified excluded IPv6 prefix from the list.

Default n/a

Parameters *ipv6-prefix/prefix-length* — a valid IPv6 address prefix

Values *ipv6-prefix* — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 to FFFF]H
d: [0 to 255]D
prefix-length — 1 to 128

5.7.2.2 Show Commands

Note: The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

ip

Syntax **ip**
ip *ip-filter-id* [**detail**]
ip *ip-filter-id* [**associations** | **counters**]
ip *ip-filter-id* **entry** *entry-id* **counters**

Context show>filter

Description This command displays IPv4 filter information.

Parameters **ip** — displays all configured IPv4 filter information

ip-filter-id — displays information for the specified filter ID or filter name and its filter entries

Values 1 to 65535 or *filter-name* (up to 64 characters)

detail — displays detailed information for the specified IPv4 filter

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

counters — displays counter information for the specified filter ID or filter entry

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

Values 1 to 65535

Output The following outputs are examples of IP filter information:

- IP filter information (Output Example, Table 84)
- IP filter information with filter ID specified (Output Example, Table 85)
- IP filter associations (Output Example, Table 86)
- IP filter counters (Output Example, Table 87)

Output Example

```
*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
```

Table 84 Filter Field Descriptions

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

Output Example

```
*A:7705:Dut-D# show filter ip 65535
===============================================================================
IP Filter
===============================================================================
Filter Id           : 65535                       Applied        : No
Scope               : Template                    Def. Action    : Drop
Entries             : 3
Sub-Entries         : 35
Description         : Description for Ip Filter Policy id # 65535
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry               : 64
Description         : Description for Ip Filter Policy id # 65535 entry 64
Log Id              : 102
Src. IP             : ip-prefix-list "prefList2"
Src. Port           : n/a
Dest. IP            : ip-prefix-list "prefList1"
Dest. Port          : n/a
Protocol            : Undefined                   Dscp           : Undefined
ICMP Type           : Undefined                   ICMP Code      : Undefined
Fragment            : Off
Sampling            : Off                         Int. Sampling  : On
IP-Option           : 0/0                         Multiple Option: Off
TCP-syn             : Off                         TCP-ack        : Off
Option-pres         : Off
Primary Action      : Forward
Ing. Matches        : 0 pkts
Egr. Matches        : 0 pkts

Entry               : 128
```

```
Description         : Description for Ip Filter Policy id # 65535 entry 128
Log Id              : 105
Src. IP             : ip-prefix-list "prefList2"
Src. Port           : n/a
Dest. IP            : ip-prefix-list "prefList1"
Dest. Port          : n/a
Protocol            : Undefined                    Dscp           : Undefined
ICMP Type           : Undefined                    ICMP Code      : Undefined
Fragment            : Off
Sampling            : Off                          Int. Sampling  : On
IP-Option           : 0/0                          Multiple Option: Off
TCP-syn             : Off                          TCP-ack        : Off
Option-pres         : Off
Primary Action      : Forward
Ing. Matches        : 0 pkts
Egr. Matches        : 0 pkts

Entry               : 256
Description         : Description for Ip Filter Policy id # 65535 entry 256
Log Id              : 199
Src. IP             : ip-prefix-list "prefList"
Src. Port           : n/a
Dest. IP            : 0.0.0.0/0
Dest. Port          : n/a
Protocol            : Undefined                    Dscp           : Undefined
ICMP Type           : Undefined                    ICMP Code      : Undefined
Fragment            : Off
Sampling            : Off                          Int. Sampling  : On
IP-Option           : 0/0                          Multiple Option: Off
TCP-syn             : Off                          TCP-ack        : Off
Option-pres         : Off
Primary Action      : Forward
Ing. Matches        : 0 pkts
Egr. Matches        : 0 pkts
===============================================================================
```

Table 85 **Filter Field Descriptions (Filter ID Specified)**

Label	Description
IP Filter	
Filter Id	The IP filter policy ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Scope	Template — the filter policy is of type template
	Exclusive — the filter policy is of type exclusive
Def. Action	The default action for packets that do not match the filter entries, either drop or forward
Entries	The number of entries configured in this filter ID

Table 85 **Filter Field Descriptions (Filter ID Specified) (Continued)**

Label	Description
Sub-Entries	The number of sub-entries configured in this filter ID
Description	The IP filter policy description, if specified
Filter Match Criteria	
Entry	The filter entry ID; Inactive indicates that the filter entry is incomplete because no action has been specified.
Description	The IP filter policy description, if specified
Log Id	The filter log identifier
Src. IP	The source IP address, IP address and prefix length, or referenced prefix match list match criterion; 0.0.0.0/0 indicates that no criterion is specified for the filter entry
Src. Port	The source TCP or UDP port match criterion
Dest. IP	The destination IP address, IP address and prefix length, or referenced prefix match list match criterion; 0.0.0.0/0 indicates that no criterion is specified for the filter entry
Dest. Port	The destination TCP or UDP port match criterion
Protocol	The protocol ID for the match criterion; Undefined indicates that no protocol is specified (IPv4 filters only)
Dscp	The DSCP name to be used as match criterion; Undefined indicates that no DSCP name is specified
ICMP Type	The ICMP type match criterion; Undefined indicates that no ICMP type is specified
ICMP Code	The ICMP code match criterion; Undefined indicates that no ICMP code is specified
Fragment (IPv4 filters only	Off — configures a match on all unfragmented packets
	On — configures a match on all fragmented packets
Next Header	The next header ID used for the match criterion; Undefined indicates that no next header is specified (IPv6 filters only)
Option-pres (IPv4 filters only	Off — does not search for packets that contain the option field or have an option field of zero
	On — matches packets that contain the option field or have an option field of zero

Table 85 **Filter Field Descriptions (Filter ID Specified) (Continued)**

Label	Description
Sampling	Off — specifies that traffic sampling is disabled
	On — specifies that traffic sampling is enabled
Int. Sampling	Off — specifies that interface traffic sampling is disabled
	On — specifies that interface traffic sampling is enabled
IP-Option	Specifies matching packets with a specific IP option or range of IP options in the IP header for IP filter match criteria
Multiple Option (IPv4 filters only	Off — the option fields are not checked
	On — packets containing one or more option fields in the IP header will be used as IP filter match criteria
TCP-syn	Off — the SYN bit is not matched
	On — matches the SYN bit being set or reset in the control bits of the TCP header of an IP packet
TCP-ack	Off — the ACK bit is not matched
	On — matches the ACK bit being set or reset in the control bits of the TCP header of an IP packet
Primary Action	Forward — the primary action for packets that do not match the filter entries is to forward
	Drop — the primary action for packets that do not match the filter entries is to drop
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Egr. Matches	The number of egress filter matches/hits for the filter entry

Output Example

```
*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     : 10.0.0.0/0                       Dest. Port     : None
Protocol     : 2                                Dscp           : Undefined
ICMP Type    : Undefined                        ICMP Code      : Undefined
Fragment     : Off                              Option-present : Off
Sampling     : Off                              Int. Sampling  : On
IP-Option    : 0/0                              Multiple Option: Off
TCP-syn      : Off                              TCP-ack        : Off
Match action : Drop
Ing. Matches : 0                                Egr. Matches   : 0
===============================================================================
*A-ALU-49#

*A-ALU-49# show filter ip 1 associations
===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 1                                Applied        : No
Scope        : Template                         Def. Action    : Drop
Entries      : 1
Description  : (Not Specified)
-------------------------------------------------------------------------------
Filter Association : IPv6
-------------------------------------------------------------------------------
No Match Found
===============================================================================
*A-ALU-49#
```

Table 86 Filter Associations Field Descriptions

Label	Description
IP Filter/IPv6 Filter	
Filter Id	The IP filter policy ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Scope	Template — the filter policy is of type template
	Exclusive — the filter policy is of type exclusive
Def. Action	The default action for packets that do not match the filter entries, either drop or forward
Entries	The number of entries configured for this filter policy
Description	The IP filter policy description, if specified
Filter Association	IP or IPv6

Table 86 **Filter Associations Field Descriptions (Continued)**

Label	Description
Filter Match Criteria: IP or IPv6	
Entry	The filter entry ID; Inactive indicates that the filter entry is incomplete because no action has been specified
Log Id	The filter log identifier
Src. IP	The source IP address, IP address and prefix length, or referenced prefix match list match criterion; 0.0.0.0/0 indicates that no criterion is specified for the filter entry
Src. Port	The source TCP or UDP port match criterion
Dest. IP	The destination IP address, IP address and prefix length, or referenced prefix match list match criterion; 0.0.0.0/0 indicates that no criterion is specified for the filter entry
Dest. Port	The destination TCP or UDP port match criterion
Protocol	The protocol ID for the match criterion; Undefined indicates that no protocol is specified (IPv4 filters only)
Dscp	The DSCP name to be used as match criterion; Undefined indicates that no DSCP name is specified
ICMP Type	The ICMP type match criterion; Undefined indicates that no ICMP type is specified
ICMP Code	The ICMP code to be used as a match criterion; Undefined indicates that no ICMP code is specified
Fragment (IPv4 filters only)	Off — configures a match on all unfragmented packets
	On — configures a match on all fragmented packets
Option-present (IPv4 filters only)	Off — does not search for packets that contain the option field or have an option field of zero
	On — matches packets that contain the option field or have an option field of zero
Sampling	Off — specifies that traffic sampling is disabled
	On — specifies that traffic sampling is enabled
Int. Sampling	Off — specifies that interface traffic sampling is disabled
	On — specifies that interface traffic sampling is enabled
IP-Option	Specifies matching packets with a specific IP option or range of IP options in the IP header for IP filter match criteria

Table 86 **Filter Associations Field Descriptions (Continued)**

Label	Description
Multiple Option (IPv4 filters only)	Off — the option fields are not checked
	On — packets containing one or more option fields in the IP header will be used as IP filter match criteria
TCP-syn	Off — the SYN bit is not matched
	On — matches the SYN bit being set or reset in the control bits of the TCP header of an IP packet
TCP-ack	Off — the ACK bit is not matched
	On — matches the ACK bit being set or reset in the control bits of the TCP header of an IP packet
Next Header	The next header ID for the match criteria; Undefined indicates that no next header is specified (IPv6 filters only)
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
Egr. Matches	The number of egress filter matches/hits for the filter entry

Output Example

```
*A-ALU-1# show filter ip 3 counters
===============================================================================
IP Filter : 100
===============================================================================
Filter Id    : 3                              Applied         : Yes
Scope        : Template                       Def. Action     : Drop
Entries      : Not Available
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry        : 10
Ing. Matches: 749                             Egr. Matches    : 0

Entry        : 200
Ing. Matches: 0                               Egr. Matches    : 0

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

```
*A-ALU-1# show filter ipv6 1 counters
===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 1                                Applied        : No
Scope        : Template                         Def. Action    : Drop
Entries      : 1
Description  : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry        : 1 (Inactive)
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

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

Table 87 Filter Counters Field Descriptions

Label	Description
IP Filter/IPv6 Filter	
Filter Id	The IP filter policy ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Scope	Template — the filter policy is of type template
	Exclusive — the filter policy is of type exclusive
Def. Action	The default action for packets that do not match the filter entries, either drop or forward
Entries	The number of entries configured in this filter ID
Description	The IP filter policy description, if specified
Filter Match Criteria: IP/IPv6	
Entry	The filter entry ID; Inactive indicates that the filter entry is incomplete because no action has been specified
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Egr. Matches	The number of egress filter matches/hits for the filter entry

ip-exception

Syntax **ip-exception**
ip-exception *ip-filter-id*
ip-exception *ip-filter-id* [**associations** | **counters**]
ip-exception *ip-filter-id* **entry** *entry-id* **counters**

Context show>filter

Description This command shows IPv4 exception filter information.

Parameters **ip-exception** — displays all configured IPv4 exception filter information

ip-filter-id — displays information for the specified IPv4 exception filter

Values 1 to 65535 or *filter-name* (up to 64 characters)

associations — appends information as to where the specified IPv4 exception filter is applied to the detailed IPv4 exception filter output

counters — displays counter information for the specified IPv4 exception filter or filter entry

entry-id — displays information for the specified IPv4 exception filter entry ID only

Values 1 to 65535

Output The following output is an example of IP exception information with a specified *ip-filter-id*, and Table 88 describes the fields.

Output Example

```
*A:7705:Dut-D# show filter ip-exception 99
===============================================================================
IP Exception Filter
===============================================================================
Filter Id           : 99                            Applied        : No
Scope               : Template
Entries             : 1
Sub-Entries         : 51
Description         : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry               : 1
Description         : (Not Specified)
Src. IP             : ip-prefix-list "prefList1"
Src. Port           : n/a
Dest. IP            : ip-prefix-list "prefList"
Dest. Port          : n/a
Protocol            : Undefined
ICMP Type           : Undefined                     ICMP Code      : Undefined
Sampling            : Off                           Int. Sampling  : On
Primary Action      : Drop
Ing. Matches        : 0 pkts
Egr. Matches        : 0 pkts
```

Table 88 **IP Exception Field Descriptions**

Label	Description
IP Exception Filter	
Filter Id	The IP exception filter policy ID
Applied	No — the IP exception filter ID has not been applied
	Yes — the IP exception filter ID is applied
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
Sub-Entries	The number of sub-entries configured in this filter ID
Description	The IP filter policy description, if specified
Filter Match Criteria: IP	
Entry	The number of entries configured in this filter ID
Description	The IP filter policy entry description string, if specified
Src. IP	The source IP address, IP address and prefix length, or referenced prefix match list match criterion; 0.0.0.0/0 indicates that no criterion is specified for the filter entry
Src. Port	The source TCP or UDP port match criterion
Dest. IP	The destination IP address, IP address and prefix length, or referenced prefix match list match criterion; 0.0.0.0/0 indicates that no criterion is specified for the filter entry
Dest. Port	The destination TCP or UDP port match criterion
Protocol	The protocol ID for the match criterion; Undefined indicates that no protocol is specified (IPv4 filters only)
ICMP Type	The ICMP type match criterion; Undefined indicates that no ICMP type is specified
ICMP Code	The ICMP code to be used as a match criterion; Undefined indicates that no ICMP code is specified
Sampling	Off — specifies that traffic sampling is disabled
	On — specifies that traffic sampling is enabled
Int. Sampling	Off — specifies that interface traffic sampling is disabled
	On — specifies that interface traffic sampling is enabled

Table 88 **IP Exception Field Descriptions (Continued)**

Label	Description
Primary Action	Forward — the primary action for packets that do not match the filter entries is to forward
	Drop — the primary action for packets that do not match the filter entries is to drop
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Egr. Matches	The number of egress filter matches/hits for the filter entry

ipv6

Syntax **ipv6**
ipv6 *ipv6-filter-id* [**detail**]
ipv6 *ipv6-filter-id* [**associations** | **counters**]
ipv6 *ipv6-filter-id* **entry** *entry-id* **counters**

Context show>filter

Description This command displays IPv6 filter information.

Parameters **ipv6** — displays all configured IPv6 filter information

ipv6-filter-id — displays information for the specified filter ID or filter name and its filter entries

Values 1 to 65535 or *filter-name* (up to 64 characters)

detail — displays detailed information for the specified IPv6 filter

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

counters — displays counter information for the specified filter ID or filter entry

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

Values 1 to 65535

Output The following outputs are examples of IPv6 filter information:

- IPv6 filter information with filter ID specified (Output Example, Table 89)
- detailed IPv6 filter information with filter ID specified (Output Example, Table 90)

Output Example

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

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

Table 89 IPv6 Filter Field Descriptions (Filter ID Specified)

Label	Description
IPv6 Filter	
Filter Id	The IPv6 filter policy ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Scope	Template — the filter policy is of type template
	Exclusive — the filter policy is of type exclusive
Def. Action	The default action for packets that do not match the filter entries, either drop or forward
Entries	The number of entries configured for this filter policy
Description	The filter policy description, if specified
Filter Match Criteria: IPv6	
Entry	The filter entry ID
Description	The IP filter policy description, if specified

Table 89 **IPv6 Filter Field Descriptions (Filter ID Specified) (Continued)**

Label	Description
Log Id	Not applicable for IPv6 filter policies
Src. IP	The source IP address, IP address and prefix length, or referenced prefix match list match criterion
Src. Port	The source TCP or UDP port match criterion
Dest. IP	The destination IP address, IP address and prefix length, or referenced prefix match list match criterion
Dest. Port	The destination TCP or UDP port match criterion
Next Header	The next header ID for the match criteria; Undefined indicates no next header is specified
Dscp	The DSCP name to be used as match criterion; Undefined indicates that no DSCP name is specified
ICMP Type	The ICMP type match criterion; Undefined indicates that no ICMP type is specified
ICMP Code	The ICMP code to be used as a match criterion; Undefined indicates that no ICMP code is specified
TCP-syn	Off — the SYN bit is not matched
	On — matches the SYN bit being set or reset in the control bits of the TCP header of an IP packet
TCP-ack	Off — the ACK bit is not matched
	On — matches the ACK bit being set or reset in the control bits of the TCP header of an IP packet
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 (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
Egr. Matches	The number of egress filter matches/hits for the filter entry

Output Example

```
*A:7705:Dut-D# show filter ipv6 1 detail
===============================================================================
IPv6 Filter
===============================================================================
Filter Id           : 1                             Applied        : No
Scope               : Template                      Def. Action    : Drop
Entries             : 1
Sub-Entries         : 64
Description         : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry               : 1
Description         : (Not Specified)
Log Id              : n/a
Src. IP             : ::/0
Src. Port           : n/a
Dest. IP            : ipv6-prefix-list "prefList"
Dest. Port          : n/a
Next Header         : Undefined                     Dscp           : Undefined
ICMP Type           : Undefined                     ICMP Code      : Undefined
Sampling            : Off                           Int. Sampling  : On
TCP-syn             : Off                           TCP-ack        : Off
Flow-label          : n/a                           Flow-label Mask: n/a
Primary Action      : Forward
Ing. Matches        : 0 pkts
Egr. Matches        : 0 pkts
-------------------------------------------------------------------------------
Filter Match IPv6 Prefix Lists
-------------------------------------------------------------------------------
ipv6-prefix-list "prefList"
===============================================================================
configured prefixes:
-------------------------------------------------------------------------------
    3000:20:10::/64
-------------------------------------------------------------------------------
generated prefixes:
-------------------------------------------------------------------------------
    3000:20:10::/123                    3000:20:10::21/128
    3000:20:10::22/127                  3000:20:10::24/126
    3000:20:10::28/125                  3000:20:10::30/124
    3000:20:10::40/122                  3000:20:10::80/121
    3000:20:10::100/120                 3000:20:10::200/119
    3000:20:10::400/118                 3000:20:10::800/117
    3000:20:10::1000/116                3000:20:10::2000/115
    3000:20:10::4000/114                3000:20:10::8000/113
    3000:20:10::1:0/112                 3000:20:10::2:0/111
    3000:20:10::4:0/110                 3000:20:10::8:0/109
    3000:20:10::10:0/108                3000:20:10::20:0/107
    3000:20:10::40:0/106                3000:20:10::80:0/105
    3000:20:10::100:0/104               3000:20:10::200:0/103
    3000:20:10::400:0/102               3000:20:10::800:0/101
    3000:20:10::1000:0/100              3000:20:10::2000:0/99
    3000:20:10::4000:0/98               3000:20:10::8000:0/97
    3000:20:10::1:0:0/96                3000:20:10::2:0:0/95
    3000:20:10::4:0:0/94                3000:20:10::8:0:0/93
    3000:20:10::10:0:0/92               3000:20:10::20:0:0/91
```

```
    3000:20:10::40:0:0/90                3000:20:10::80:0:0/89
    3000:20:10::100:0:0/88               3000:20:10::200:0:0/87
    3000:20:10::400:0:0/86               3000:20:10::800:0:0/85
    3000:20:10::1000:0:0/84              3000:20:10::2000:0:0/83
    3000:20:10::4000:0:0/82              3000:20:10::8000:0:0/81
    3000:20:10:0:1::/80                  3000:20:10:0:2::/79
    3000:20:10:0:4::/78                  3000:20:10:0:8::/77
    3000:20:10:0:10::/76                 3000:20:10:0:20::/75
   3000:20:10:0:40::/74                 3000:20:10:0:80::/73
    3000:20:10:0:100::/72                3000:20:10:0:200::/71
    3000:20:10:0:400::/70                3000:20:10:0:800::/69
    3000:20:10:0:1000::/68               3000:20:10:0:2000::/67
   3000:20:10:0:4000::/66               3000:20:10:0:8000::/65
-------------------------------------------------------------------------------
NUM prefixes: 65
References:
-------------------------------------------------------------------------------
    IPv6-filter 1      entry 1      Dst-Ip
-------------------------------------------------------------------------------
NUM references: 1
NUM IPv6 Prefix Lists: 1
-------------------------------------------------------------------------------
Filter Match Port Lists
-------------------------------------------------------------------------------
No Port Lists
===============================================================================
```

Table 90 **Detailed IPv6 Filter Field Descriptions (Filter ID Specified)**

Label	Description
IPv6 Filter	
Filter Id	The filter policy ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Scope	Template — the filter policy is of type template
	Exclusive — the filter policy is of type exclusive
Def. Action	The default action for packets that do not match the filter entries, either drop or forward
Entries	The number of entries configured for this filter policy
Description	The filter policy description, if specified
Filter Match Criteria: IPv6	
Entry	The filter entry ID
Description	The filter policy description; if no description is assigned, (Not Specified) is displayed

Table 90 **Detailed IPv6 Filter Field Descriptions (Filter ID Specified)**

Label	Description
Log Id	Not applicable for IPv6 filter policies
Src. IP	The source IP address, IP address and prefix length, or referenced prefix match list match criterion
Src. Port	The source TCP or UDP port match criterion
Dest. IP	The destination IP address, IP address and prefix length, or referenced prefix match list match criterion
Dest. Port	The destination TCP or UDP port match criterion
Next Header	The next header ID for the match criteria; Undefined indicates no next header is specified
Dscp	The DSCP name to be used as match criterion; Undefined indicates that no DSCP name is specified
ICMP Type	The ICMP type match criterion; Undefined indicates that no ICMP type is specified
ICMP Code	The ICMP code to be used as a match criterion; Undefined indicates that no ICMP code is specified
Sampling	Off — specifies that traffic sampling is disabled
	On — specifies that traffic sampling is enabled
Int. Sampling	Off — specifies that interface traffic sampling is disabled
	On — specifies that interface traffic sampling is enabled
TCP-syn	Off — the SYN bit is not matched
	On — matches the SYN bit being set or reset in the control bits of the TCP header of an IP packet
TCP-ack	Off — the ACK bit is not matched
	On — matches the ACK bit being set or reset in the control bits of the TCP header of an IP packet
Flow-label	Not applicable for IPv6 filters
Flow-label Mask	Not applicable for IPv6 filters
Primary Action	Forward — the primary action for packets that do not match the filter entries is to forward
	Drop — the primary action for packets that do not match the filter entries is to drop

Table 90 **Detailed IPv6 Filter Field Descriptions (Filter ID Specified)**

Label	Description
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Egr. Matches	The number of egress filter matches/hits for the filter entry
Filter Match IPv6 Prefix Lists	
ipv6-prefix-list	The prefix list name
configured prefixes	The address and prefix length of the configured prefixes
generated prefixes	The address and prefix length of the generated prefixes
NUM prefixes	The total number of configured and generated prefixes
References	The policies, policy entries, and source/destination IPv6 match type per entry referring to the specified match list
NUM references	The total number of configured references
NUM IPv6 Prefix Lists	The total number of configured IPv6 prefix lists
Filter Match Port Lists	Not applicable for the 7705 SAR

log

Syntax **log** [**bindings**]
log *log-id* [**match** *string*]

Context show>filter

Description This command displays filter log information.When a filter **log** command is used with a MAC filter and a packet is matched, the log entry is different from an IP filter entry. For a MAC filter, the source and destination IP address of incoming packets are not included in the log.

Parameters **bindings** — displays the number of filter logs currently available

log-id — the filter log ID destination expressed as a decimal integer

Values 101 to 199

string — specifies to display the log entries starting from the first occurrence of the specified string

Values up to 32 characters

Output The following outputs are examples of filter log information:

- filter log information (Output Example, Table 91)
- filter log bindings (Output Example, Table 92)

Output Example

```
*A-ALU-1# show filter log
===============================================================================
Filter Logs
===============================================================================
Log-Id Dest.  Id/Entries Enabled Description
-------------------------------------------------------------------------------
101    Memory 1000       Yes     Default filter log
       Wrap: Enabled
1 Entries Found
===============================================================================
*A-ALU-1#


*A-ALU-1# show filter log 101
===============================================================================
Filter Log
===============================================================================
Admin state : Enabled
Description : Default filter log
Destination : Memory
Wrap        : Enabled
-------------------------------------------------------------------------------
Maximum entries configured : 1000
Number of entries logged   : 4
2011/1124 22:10:03  Ip Filter: 1:12  Desc: Descr. for Ip Fltr Policy id # 1 entry 12
SDP: 1:60000  Direction: Ingress  Action: Drop
Src MAC: 1f-ff-f0-1f-ff-c5  Dst MAC: aa-bb-cc-dd-ee-ff  EtherType: 0800
Src IP: 10.50.1.144:3216  Dst IP: 10.10.11.2:0  Flags: 0  TOS: b8  TTL: 64
Protocol: UDP

2011/1124 22:10:03  Ip Filter: 1:12  Desc: Descr. for Ip Fltr Policy id # 1 entry 12
SDP: 1:60000  Direction: Ingress  Action: Drop
Src MAC: 1f-ff-f0-1f-ff-c5  Dst MAC: aa-bb-cc-dd-ee-ff  EtherType: 0800
Src IP: 10.50.1.144:3216  Dst IP: 10.10.11.2:0  Flags: 0  TOS: b8  TTL: 64
Protocol: UDP

2011/1124 22:10:06  Ip Filter: 1:13  Desc: Descr. for Ip Fltr Policy id # 1 entry 13
SDP: 1:60000  Direction: Ingress  Action: Drop
Src MAC: 1f-ff-f0-1f-ff-c5  Dst MAC: aa-bb-cc-dd-ee-ff  EtherType: 0800
Src IP: 10.50.1.16:0  Dst IP: 10.10.11.2:31  Flags: 0  TOS: b8  TTL: 64
Protocol: UDP

2011/1124 22:10:06  Ip Filter: 1:13  Desc: Descr. for Ip Fltr Policy id # 1 entry 13
SDP: 1:60000  Direction: Ingress  Action: Drop
Src MAC: 1f-ff-f0-1f-ff-c5  Dst MAC: aa-bb-cc-dd-ee-ff  EtherType: 0800
Src IP: 10.50.1.16:0  Dst IP: 10.10.11.2:31  Flags: 0  TOS: b8  TTL: 64
Protocol: UDP

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

Table 91 **Filter Log Field Descriptions**

Label	Description
Log-Id	The filter log ID
Dest./Destination	The destination of the filter log: memory or syslog
Id/Entries	The number of entries configured for this filter log
Enabled	Indicates whether the log is administratively enabled
Admin State	The administrative state of the log: enabled or disabled
Description	The description string configured for the filter log
Wrap	Indicates whether the wraparound function (circular buffer) is enabled
Maximum entries configured	The maximum number of entries allowed in this filter log
Number of entries logged	The number of entries in this filter log
(*date*)	The timestamp of the entry
Ip Filter	The filter ID and entry ID
Desc.	The description string for the filter log
SDP	The SDP using this filter
Direction	The direction of the traffic being filtered
Action	The action taken as a result of the filter
Src MAC	The source MAC address of the packet
Dst MAC	The destination MAC address of the packet
EtherType	The Ethertype of the packet
Src IP	The source IP address of the packet
Dst IP	The destination IP address of the packet
Flags	The number of flags associated with the packet
TOS	The type of service for the packet expressed as a hexadecimal number. Use the **show>qos>dscp-table** command to see the definitions of the numbers.
TTL	The time to live setting remaining for the packet
Protocol	The protocol used for the packet

Output Example

```
*A-ALU-1# show filter log bindings

===============================================================================
Filter Log Bindings
===============================================================================
Total Log Instances (Allowed)          : 2047
Total Log Instances (In Use)           : 1
Total Log Bindings                     : 1

-------------------------------------------------------------------------------
Type  FilterId EntryId   Log    Instantiated
-------------------------------------------------------------------------------
 Cpm         1       2   101             Yes

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

Table 92 **Filter Log Bindings Field Descriptions**

Label	Description
Total Log Instances (Allowed)	The maximum allowed instances of filter logs allowed on the system
Total Log Instances (In Use)	The instances of filter logs presently existing on the system
Total Log Bindings	The count of the filter log bindings presently existing on the system
Type	The type of filter: CPM, IP, or MAC
FilterID	The unique identifier of the filter
EntryID	The unique identifier of an entry in the filter table
Log	The filter log identifier
Instantiated	Specifies if the filter log for this filter entry has been enabled

mac

Syntax **mac** {*mac-filter-id* [**entry** *entry-id*] [**associations** | **counters**]}

Context show>filter

Description This command displays MAC filter information.

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

Values 1 to 65535 or *filter-name* (up to 64 characters)

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

Values 1 to 65535

associations — displays information on where the filter policy ID is applied to the detailed filter policy ID output

counters — displays counter information for the specified filter ID

Output The following outputs are examples of MAC filter information:

- no parameters specified (Output Example, Table 93)
- *mac-filter-id* specified (Output Example, Table 94)
- associations specified (Output Example, Table 95)
- counters specified (Output Example, Table 96)

Output Example

When no parameters are specified, a brief listing of MAC filters is produced.

```
*A-ALU-1>show>filter# mac
===============================================================================
Mac Filters                                                        Total:     3
===============================================================================
Filter-Id Scope    Applied Description
-------------------------------------------------------------------------------
11        Template No
232       Template Yes     filter-west
5000      Template No
-------------------------------------------------------------------------------
Num MAC filters: 3
===============================================================================
*A-ALU-1#
```

Table 93 **Filter MAC Field Descriptions (No Filter ID Specified)**

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

Output Example

When the filter ID is specified, detailed filter information for the filter ID and its entries is displayed.

```
*A-ALU-1# show filter# mac 5000
===============================================================================
Mac Filter
===============================================================================
Filter Id    : 5000                             Applied         : No
Scope        : Template                         Def. Action     : Drop
Entries      : 1
Description : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
-------------------------------------------------------------------------------
Entry        : 5000 (Inactive)                  FrameType       : Ethernet
Description : (Not Specified)
Log Id       : n/a
Src Mac      : ff:ff:ff:ff:ff:ff
Dest Mac     :
Dot1p        : Undefined                        Ethertype       : Undefined
DSAP         : Undefined                        SSAP            : Undefined
Snap-pid     : Undefined                        ESnap-oui-zero  : Undefined
Match action: Drop
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

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

Table 94 **Filter MAC Field Descriptions (Filter ID Specified)**

Label	Description
MAC Filter	
Filter Id	The MAC filter policy ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Def. Action	Forward — the default action for the filter ID for packets that do not match the filter entries is to forward
	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop
Entries	The number of entries in the filter policy

Table 94 **Filter MAC Field Descriptions (Filter ID Specified) (Continued)**

Label	Description
Description	The MAC filter policy description
Filter Match Criteria: Mac	
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
FrameType	Ethernet — the entry ID match frame type is Ethernet IEEE 802.3
	Ethernet II — the entry ID match frame type is Ethernet Type II.
Description	The filter entry description
Log Id	The filter log identifier
Src Mac	The source MAC address match criterion. If the MAC address is all zeros, no criterion is specified for the filter entry.
Dest Mac	The destination MAC address match criterion. If the MAC address is all zeros, no criterion is specified for the filter entry.
Dot1p	The IEEE 802.1p value for the match criterion. Undefined indicates that no value is specified
Ethertype	The Ethertype value match criterion
DSAP	The DSAP value match criterion. Undefined indicates that no value is specified
SSAP	The SSAP value match criterion. Undefined indicates that no value is specified
Snap-pid	The Ethernet SNAP PID value match criterion. Undefined indicates that no value is specified
Esnap-oui-zero	Non-Zero — filter entry matches a non-zero value for the Ethernet SNAP OUI
	Zero — filter entry matches a zero value for the Ethernet SNAP OUI
	Undefined — no Ethernet SNAP OUI value is specified

Table 94 **Filter MAC Field Descriptions (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 the entry is Inactive, the filter entry is incomplete, no action was specified
	Drop — packets matching the filter entry criteria will be dropped
	Forward — packets matching the filter entry criteria are forwarded
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Egr. Matches	The number of egress filter matches/hits for the filter entry

Output Example

```
*A-ALU-1# show filter# mac 11 associations
===============================================================================
Mac Filter
===============================================================================
Filter Id    : 11                               Applied         : No
Scope        : Template                         Def. Action     : Drop
Entries      : 1
Description : (Not Specified)
-------------------------------------------------------------------------------
Filter Association : Mac
-------------------------------------------------------------------------------
No Match Found
===============================================================================
```

Table 95 **Filter MAC Associations Field Descriptions**

Label	Description
Filter Id	The IP filter ID
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Entries	The number of entries in the filter
Description	The MAC filter policy description
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied

Table 95 **Filter MAC Associations Field Descriptions (Continued)**

Label	Description
Def. Action	Forward — the default action for the filter ID for packets that do not match the filter entries is to forward
	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop
Filter Association	The type of filter association

Output Example

```
*A-ALU-1# show filter# mac 11 counters
===============================================================================
Mac Filter
===============================================================================
Filter Id    : 11                               Applied         : No
Scope        : Template                         Def. Action     : Drop
Entries      : 1
Description : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
-------------------------------------------------------------------------------
Entry        : 11 (Inactive)                    FrameType       : Ethernet II
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

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

Table 96 **Filter MAC Counters Field Descriptions**

Label	Description
Filter Id	The IP filter ID
Scope	Template — the filter policy is of type Template
	Exclusive — the filter policy is of type Exclusive
Entries	The number of entries in the filter
Description	The MAC filter policy description
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Def. Action	Forward — the default action for the filter ID for packets that do not match the filter entries is to forward
	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop

Table 96 **Filter MAC Counters Field Descriptions (Continued)**

Label	Description
Filter Match Criteria: Mac	
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
FrameType	Ethernet — the entry ID match frame type is Ethernet IEEE 802.3
	Ethernet II — the entry ID match frame type is Ethernet Type II
Ing. Matches	The number of ingress filter matches/hits for the filter entry
Egr. Matches	The number of egress filter matches/hits for the filter entry

match-list

Syntax **match-list**

Context show>filter

Description This command enables the context to display information for match lists used in IPv4, IPv6, IP exception, CSM, or management access filter policies.

ip-prefix-list

Syntax **ip-prefix-list** [*prefix-list-name*]
ip-prefix-list *prefix-list-name* **references**

Context show>filter>match-list

Description This command displays IPv4 prefix information for match criteria in filter policies.

Parameters *prefix-list-name* — the name of a configured IPv4 prefix match list

references — displays the filter policies, policy entries, and source/destination IPv4 match type per entry referring to the specified match list

Output The following outputs are examples of filter match list information:

- when a prefix list name is specified (Output Example, Table 97)
- when **references** is used with a specified prefix list (Output Example, Table 98)
- when **prefix-exclude** is used to exclude IPv4 prefixes from an IP prefix list (Output Example, Table 99)

Output Example

When a prefix list name is specified:

```
*A:7705:Dut-D# show filter match-list ip-prefix-list "prefList1"
===============================================================================
Filter Match IP Prefix Lists
===============================================================================
ip-prefix-list "prefList1"
===============================================================================
configured prefixes:
-------------------------------------------------------------------------------
    100.1.1.1/32       100.1.1.2/32       100.1.1.3/32
-------------------------------------------------------------------------------
NUM prefixes: 3
References:
-------------------------------------------------------------------------------
   IP-filter 65535    entry 64     Dst-Ip
   IP-filter 65535    entry 128    Dst-Ip
   IP Exception-filt*
-------------------------------------------------------------------------------
NUM references: 3
===============================================================================
```

Table 97 **Filter Match List Field Descriptions (IPv4 Prefix List Name Specified)**

Label	Description
Filter Match IP Prefix Lists	
ip-prefix-list	The prefix list name
configured prefixes	The address and prefix length of the configured prefixes
NUM prefixes	The total number of configured prefixes
References	The policies, policy entries, and source/destination IPv4 match type per entry referring to the specified match list
NUM references	The total number of configured references

Output Example

When **references** is used with a specified prefix list name:

```
*A:7705:Dut-D# show filter match-list ip-prefix-list "prefList1" references
===============================================================================
Filter Match IP Prefix Lists
===============================================================================
ip-prefix-list "prefList1"
===============================================================================
References:
-------------------------------------------------------------------------------
    IP-filter 65535    entry 64     Dst-Ip
    IP-filter 65535    entry 128    Dst-Ip
    IP Exception-filt*
```

```
-------------------------------------------------------------------------------
NUM references: 3
===============================================================================
```

Table 98 **Filter Match List Field Descriptions (IPv4 Prefix List Name and References Specified)**

Label	Description
Filter Match IP Prefix Lists	
ip-prefix-list	The prefix list name
References	The policies, policy entries, and source/destination IPv4 match type per entry referring to the specified match list
NUM references	The total number of configured references

Output Example

When **prefix-exclude** is used to exclude IPv4 prefixes from an IP prefix list:

```
A:7705:Dut-D# show filter match-list ip-prefix-list "prefList"
===============================================================================
Filter Match IP Prefix Lists
===============================================================================
ip-prefix-list "prefList"
===============================================================================
configured prefixes:
-------------------------------------------------------------------------------
    100.100.0.0/24     100.200.0.0/24     100.200.1.0/24
-------------------------------------------------------------------------------
generated prefixes:
-------------------------------------------------------------------------------
    100.100.0.0/28     100.100.0.16/29    100.100.0.28/30    100.100.0.32/29
    100.100.0.44/30    100.100.0.48/28    100.100.0.64/26    100.100.0.128/25
    100.200.0.0/28     100.200.0.16/29    100.200.0.28/30    100.200.0.32/29
    100.200.0.44/30    100.200.0.48/28    100.200.0.64/26    100.200.0.128/25
-------------------------------------------------------------------------------
NUM prefixes: 19
References:
-------------------------------------------------------------------------------
    IP-filter 65535    entry 256    Src-Ip
    IP Exception-filt*
-------------------------------------------------------------------------------
NUM references: 2
===============================================================================
```

Table 99 **Filter Match List Field Descriptions (IPv4 Prefix List with Excluded Prefixes)**

Label	Description
Filter Match IP Prefix Lists	
ip-prefix-list	The prefix list name
configured prefixes	The address and prefix length of the configured prefixes
generated prefixes	The address and prefix length of the generated prefixes
NUM prefixes	The total number of configured and generated prefixes
References	The policies, policy entries, and source/destination IPv4 match type per entry referring to the specified match list
NUM references	The total number of configured references

ipv6-prefix-list

Syntax **ipv6-prefix-list** [*prefix-list-name*]
ipv6-prefix-list *prefix-list-name* **references**

Context show>filter>match-list

Description This command displays IPv6 prefix information for match criteria in filter policies.

Parameters *prefix-list-name* — the name of a configured IPv6 prefix match list

references — displays the filter policies, policy entries, and source/destination IPv6 match type per entry referring to the specified match list

Output The following outputs are examples of filter match list information:

- when an IPv6 prefix list name is specified (Output Example, Table 100)
- when **references** is used with a specified IPv6 prefix list (Output Example, Table 101)
- when **prefix-exclude** is used to exclude IPv6 prefixes from an IPv6 prefix list (Output Example, Table 102)

Output Example

When an IPv6 prefix list name is specified:

```
*A:7705:Dut-D# show filter match-list ipv6-prefix-list "prefList1"
===============================================================================
Filter Match IPv6 Prefix Lists
===============================================================================
ipv6-prefix-list "prefList1"
===============================================================================
configured prefixes:
-------------------------------------------------------------------------------
    3000:20:10::/64      3000:20:10::/123    3000:20:10::21/128
-------------------------------------------------------------------------------
NUM prefixes: 3
References:
-------------------------------------------------------------------------------
    IPv6-filter 1      entry 1      Dst-Ip
-------------------------------------------------------------------------------
NUM references: 1
===============================================================================
```

Table 100 Filter Match List Field Descriptions (IPv6 Prefix List Name Specified)

Label	Description
Filter Match IPv6 Prefix Lists	
ipv6-prefix-list	The IPv6 prefix list name
configured prefixes	The address and prefix length of the configured prefixes
NUM prefixes	The total number of configured prefixes
References	The policies, policy entries, and source/destination IPv6 match type per entry referring to the specified match list
NUM references	The total number of configured references

Output Example

When **references** is used with a specified IPv6 prefix list name:

```
*A:7705:Dut-D# show filter match-list ipv6-prefix-list "prefList1" references
===============================================================================
Filter Match IPv6 Prefix Lists
===============================================================================
ipv6-prefix-list "prefList1"
===============================================================================
References:
-------------------------------------------------------------------------------
    IPv6-filter 1      entry 1      Dst-Ip
    IPv6-filter 1      entry 24     Dst-Ip
-------------------------------------------------------------------------------
NUM references: 2
===============================================================================
```

Table 101 **Filter Match List Field Descriptions (IPv6 Prefix List Name and References Specified)**

Label	Description
Filter Match IPv6 Prefix Lists	
ipv6-prefix-list	The IPv6 prefix list name
References	The policies, policy entries, and source/destination IPv6 match type per entry referring to the specified match list
NUM references	The total number of configured references

Output Example

When **prefix-exclude** is used to exclude IPv6 prefixes from an IPv6 prefix list:

```
A:7705:Dut-D# show filter match-list ipv6-prefix-list "prefList"
===============================================================================
Filter Match IPv6 Prefix Lists
===============================================================================
ipv6-prefix-list "prefList"
===============================================================================
configured prefixes:
-------------------------------------------------------------------------------
    3000:20:10::/64
-------------------------------------------------------------------------------
generated prefixes:
-------------------------------------------------------------------------------
    3000:20:10::/123                    3000:20:10::21/128
    3000:20:10::22/127                  3000:20:10::24/126
  ...
    3000:20:10:0:10::/76                3000:20:10:0:20::/75
    3000:20:10:0:40::/74                3000:20:10:0:80::/73
    3000:20:10:0:100::/72               3000:20:10:0:200::/71
    3000:20:10:0:400::/70               3000:20:10:0:800::/69
    3000:20:10:0:1000::/68              3000:20:10:0:2000::/67
    3000:20:10:0:4000::/66              3000:20:10:0:8000::/65
-------------------------------------------------------------------------------
NUM prefixes: 65
References:
-------------------------------------------------------------------------------
    IPv6-filter 1      entry 1      Dst-Ip
-------------------------------------------------------------------------------
NUM references: 1
===============================================================================
```

Table 102 **Filter Match List Field Descriptions (IPv6 Prefix List with Excluded Prefixes)**

Label	Description
Filter Match IPv6 Prefix Lists	
ipv6-prefix-list	The IPv6 prefix list name
configured prefixes	The address and prefix length of the configured prefixes
generated prefixes	The address and prefix length of the generated prefixes
NUM prefixes	The total number of configured and generated prefixes
References	The policies, policy entries, and source/destination IPv6 match type per entry referring to the specified match list
NUM references	The total number of configured references

vlan

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

Context show>filter

Description This command displays VLAN filter information.

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

Values 1 to 65535 or *filter-name* (up to 64 characters)

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

Values 1 to 65535

Output The following outputs are examples of VLAN filter information:

- no parameters specified (Output Example, Table 103)
- *filter-id* specified (Output Example, Table 104)

Output Example

When no parameters are specified, a brief listing of VLAN filters is displayed.

```
*A-ALU-1:show>filter# vlan
===============================================================================
VLAN Filters                                                    Total:     2
===============================================================================
Filter-Id Scope     Applied   Description
-------------------------------------------------------------------------------
```

```
2         Template  Yes       VLAN_filter_2
65535     Template  No
------------------------------------------------------------------------------
Num VLAN filters: 2
==============================================================================
*A-ALU-1:show>filter#
```

Table 103 **Filter VLAN Field Descriptions (No Filter Specified)**

Label	Description
Filter-Id	The VLAN filter ID
Scope	Template — the VLAN filter policy is always of type Template
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Description	The VLAN filter policy description

Output Example

When the filter ID is specified, detailed filter information for the filter and its entries is displayed.

```
*A:7705custDoc:Sar18>show>filter# vlan 2
===============================================================================
VLAN Filter
===============================================================================
Filter Id    : 2                                Applied        : Yes
Scope        : Template                         Def. Action    : drop
Entries      : 4
Description  : VLAN_filter_2
-------------------------------------------------------------------------------
Filter Match Criteria :
-------------------------------------------------------------------------------
Entry        : 2
Description  : vlan_fltr_entry2
Match        : Untagged                         Action         : forward

Entry        : 3
Description  : vlan_fltr_entry3
Match        : VLAN                             Action         : drop
Operation    : eq
Vlan-Id      : 2

Entry        : 4
Description  : vlan_fltr_entry4
Match        : VLAN                             Action         : drop
Operation    : eq
Vlan-Id      : 445

Entry        : 65535
Description  : (Not Specified)
```

```
Match         : VLAN                                Action          : drop
Operation     : range
From          : 2000                                To              : 3000
===============================================================================
*A:7705custDoc:Sar18>show>filter#
```

Table 104 **Filter VLAN Field Descriptions (Filter ID Specified)**

Label	Description
VLAN Filter	
Filter Id	The VLAN filter policy ID
Applied	No — the filter policy ID has not been applied
	Yes — the filter policy ID is applied
Scope	Template — the filter policy is always of type Template
Def. Action	Forward — the default action for the filter ID for packets that do not match the filter entries is to forward
	Drop — the default action for the filter ID for packets that do not match the filter entries is to drop
Entries	The number of entries in the filter policy
Description	The VLAN filter policy description
Filter Match Criteria:	
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 filter entry description
Match	VLAN— the type of match criteria for the entry is VLAN
	Untagged — the type of match criteria for the entry is untagged
Action	Drop — packets matching the filter entry criteria will be dropped
	Forward — packets matching the filter entry criteria will be forwarded
Operation	The match criteria operator. Valid operators are: lt (less than), gt (greater than), eq (equal to), and range (for a range of VLAN IDs).
Vlan-Id	The VLAN ID when the match criteria defines a specific VLAN ID
From	The start VLAN ID when the match criteria defines a VLAN ID range

Table 104 **Filter VLAN Field Descriptions (Filter ID Specified) (Continued)**

Label	Description
To	The end VLAN ID when the match criteria defines a VLAN ID range

app-group

Syntax **app-group** [*group-id* | *name*] [**entry** *entry-id*] [**detail**]

Context show>security

Description This command displays firewall application group information.

Parameters *group-id* — displays information for the specified application group ID

Values 1 to 100

name — displays information for the specified application group name

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

entry-id — displays information for the specified application group entry ID

Values 1 to 65535

detail — displays detailed information on the specified application group

capture

Syntax **capture** [**format** {**decode** | **raw**}]

Context show>security

Description This command displays summary information about the captured packets stored in the debug security log.

Parameters **format decode** — the debug security log displays the packet IP header and relevant Layer 4 headers

format raw — the debug security log displays the raw packet in hexadecimal format

Output The following output is an example of captured packet information.

Output Example

```
*A-ALU-1# show security capture
===============================================================================
Security Packet Capture
===============================================================================
State          :STOPPED
Start Time     :NEVER
Running Time   : 0 days   0 hours   0 mins 0 secs
Memory Capture Contents:    [size=1024      count=0  <continuous>]

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

control-summary

Syntax **control-summary**

Context show>security

Description This command displays a summary of the receive control queues for a security zone.

Output The following output is an example of receive control queue information.

Output Example

```
*A-ALU-1# show security control-summary
===============================================================================
Zone Control Summary (Packets)
===============================================================================
Zone                                                Forwarded              Dropped
-------------------------------------------------------------------------------
VPRN_ZONE                                                   0                    0
ACCESS-POINT                                                0                    0
PUBLIC-INTERNET                                             1                    0
60                                                          0                    0
-------------------------------------------------------------------------------
Num of Zones:  4
===============================================================================
*A-ALU-1#
```

engine

Syntax **engine**

Context show>security

Description This command displays a system-level security engine statistics. During a CSM switch, security statistics roll back to zero.

Output The following output is an example of security engine statistics.

Output Example

```
*A-ALU-1# show security engine
===============================================================================
Security Engine
===============================================================================
                                                                       Packets
-------------------------------------------------------------------------------
Rx Queue
  Forwarded -  Control                                                       1
            -  Session Data                                           96932032
  Dropped                                                         19944168792

Security Processing
  Passed                                                           96932033
  Dropped                                                                 0

CPU Utilization  (Sample period:   1 sec):         100 %
===============================================================================
*A-ALU-1#
```

host-group

Syntax **host-group** [*group-id* | *name*] [**detail**]

Context show>security

Description This command displays firewall host group information.

Parameters *group-id* — displays information for the specified host group ID

Values 1 to 100

name — displays information for the specified host group name

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

detail — displays detailed information on the specified host group

log

Syntax **log** [*log-id* | *name*]
log events [**type** *event-type*]
log profile {*log-profile-id* | *name*} [**type** *event-type*]
log profiles

Context show>security

Description This command displays firewall logging information.

Parameters *log-id* — displays information for the specified log ID

Values 1 to 100

name — displays information for the specified log name or log profile name

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

event-type — displays information on the specified log event type

Values 1 to 32 characters

log-profile-id — displays information for the specified log profile ID

Values 1 to 100

events — displays information for all log events

profiles — displays information for all log profiles

Output The following output is an example of security log information, and Table 105 describes the fields.

Output Example

```
*A-ALU-1# show security log SecurityLog11
===============================================================================
Security Log: SecurityLog11
===============================================================================
Description: Security Log ID 11
Profile    : DEFAULT
Memory log contents  [size=1024   next-event=3  (wrapped)]

1 06/11/2015 17:25:56  SECURITY:Packet Base IF:ies-201-10.1.0.1
 Outbound : Forward Zone (Rule:1)
 Inbound   : GRT Zone (Rule:1)
 Session   : 1-FWD
 Report    : SessionBegin
 IP header  :
    ver:4  hlen:20  tos:0x00  len:84  hxsum:0x4fa3
    id:0x0001 frag:000 (offset:0)
   10.1.1.1->10.1.1.2   proto:ICMP
 ICMP header:
    type:8  code:0  xsum:0x059e (echo-request)

2 06/11/2015 17:26:56  SECURITY:Audit       SESSION:1
 Outbound  : <None>
 Inbound    : GRT Zone
 Session    : 1-FWD
 Report     : SessionEnd (TIMER-EXPIRED)
===============================================================================
*A-ALU-1#


*A-ALU-1# show security log events
===============================================================================
Security Logging Events
===============================================================================
Name                                    ID Severity State
-------------------------------------------------------------
PACKET
  TcpInvalidHeader                      01 INFORM   throttle
  DnsInvalidHeader                      02 INFORM   throttle
```

```
  DnsUnmatchedAnswer                    03 INFORM   throttle
...
ZONE
  NoRuleMatched                         01 INFORM   throttle
  SessionLimitReached                   02 INFORM   throttle
POLICY
  Matched                               01 INFORM   suppress
  MatchedNAT                            02 INFORM   suppress
  ActionReject                          03 INFORM   throttle
...
SESSION
  SessionBegin                          01 INFORM   throttle
  SessionEnd                            02 INFORM   throttle
  SessionBeginEnd                       03 INFORM   throttle
APPLICATION
  Summary                               01 INFORM   throttle
  HandshakeMissing                      02 INFORM   throttle
  HandshakeCtlInvalid                   03 INFORM   throttle
  HandshakeDataUnexpected               04 INFORM   throttle
...
ALG
  CmdIncomplete                         01 INFORM   throttle
  DynamicRuleInserted                   02 INFORM   throttle
  DynamicRuleInsertedPASV               03 INFORM   throttle
...
-------------------------------------------------------------
Num of Events: 61
=============================================================
```

Table 105 Security Log Field Descriptions

Label	Description
Security Logs	
Description	The security log identifier
Profile	The security logging profile to which the log applies
Memory log contents	Details of the log content
Outbound	Session location of the zone in the outbound direction
Inbound	Session location of the zone in the inbound direction
Session	The session ID
Report	The security log event code
IP header	The IPv4 packet header
Security Logging Events	
Name	The name of the event type and event
ID	The event identifier

Table 105 **Security Log Field Descriptions (Continued)**

Label	Description
Severity	The severity of the event
State	Indicates how each event is being handled

policer-group

Syntax **policer-group** [*group-id* | *name*] [**statistics**]

Context show>security

Description This command displays policer group information.

Parameters *group-id* — displays detailed information for the specified policer group ID

Values 1 to 1024

name — displays detailed information for the specified policer group name

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

statistics — displays policer group statistics when a group is specified

Output The following output is an example of policer group information.

Output Example

```
*A:7705:Dut-C# show security policer-group 1 statistics
===============================================================================
Security Policer-Group
===============================================================================
Group Id         : 1                                Applied        : Yes
Name             : policer-group 1
Description      : session rate created by SNMP
Ingress Rate     : 1 mbps
CBS (bytes)      : 1024
===============================================================================
===============================================================================
Policer Traffic Statistics
===============================================================================
                                                  Forward                Reverse
-------------------------------------------------------------------------------
Passed
  Packets                                          247690                 101822
  Octets                                         36162740               14866012
Dropped Packets
  Rate-Exceeded                                    2777461                2919967
===============================================================================
```

policing-summary

Syntax **policing-summary**

Context show>security

Description This command displays a summary of traffic statistics for policers.

Output The following output is an example of traffic statistics for policers.

Output Example

```
*A:7705:Dut-C# show security policing-summary
===============================================================================
Policing Summary (Packets)
===============================================================================
Policer                                    Forwarded                 Dropped
-------------------------------------------------------------------------------
policer-group 1                               432001                 7042904
policer-group 2                               863995                 6610910
policer-group 3                               808609                 4096798
policer-group 4                               436480                 1656494
policer-group 5                               405590                 1164140
policer-group 6                               321247                  725240
policer-group 7                               320532                  576457
policer-group 8                               336382                  488707
-------------------------------------------------------------------------------
Num of Groups: 8
===============================================================================
```

policy

Syntax **policy** [*policy-id* | *policy-name*] [**detail**] [**association**]
policy [*policy-id* | *policy-name*] [**entry** *entry-id*] [**detail**] [**association**]

Context show>security

Description This command displays security policy information.

Parameters *policy-id* — displays detailed information for the specified policy ID

Values 1 to 65535

policy-name — specifies the name of the policy

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

entry-id — displays information on the specified policy entry ID

Values 1 to 65535

detail — displays detailed information on the specified policy or filter

association — displays counter information for the specified policy or entry ID

Output The following output is an example of security policy information, and Table 106 describes the fields.

Output Example

```
*A-ALU-1# show security policy
===============================================================================
Security Policies
===============================================================================
Policy Id    Scope          Applied        Name
-------------------------------------------------------------------------------
1            Template       Yes            Inbound Policy
2            Template       Yes            IES Policy
-------------------------------------------------------------------------------
Num of Policies: 2
===============================================================================
*A-ALU-1#


*A-ALU-1# show security policy 1 detail
===============================================================================
Security Policy
===============================================================================
Policy Id    : 1                                Applied        : Yes
Name         : Inbound Policy
Scope        : Template                         Def. Action    : Reject
Entries      : 1
Description  : common egress policy
-------------------------------------------------------------------------------
Policy Match Criteria : IP
-------------------------------------------------------------------------------
Entry            : 1                                Active         : yes
Description      : match TCP and port
Match direction  : zone-inbound
Src. IP          : None                             Src. Port      : eq21
Dest. IP         : None                             Dest. Port     : None
Protocol         : tcp
ICMP Type        : Undefined                        ICMP Code      : Undefined
Profile ID       : DEFAULT                          Session        : Fwd-Dir-O*
Action           : nat                              Session Limit : None
Logging          : suppressed

Entry            : 2                                Active: Yes
Description      : match UDP and IP                 TCP-ack        : Off
Match direction  : zone-inbound
Src. IP          : 10.100.0.2                       Src. Port      : None
Dest. IP         : None                             Dest. Port     : None
Protocol         : udp
ICMP Type        : Undefined                        ICMP Code      : Undefined
Profile ID       : DEFAULT                             Session     : Bi-Direct*
Action           : reject                              Session Limit : None
Logging          : suppressed
===============================================================================
*A-ALU-1#
```

```
*A-ALU-1# show security policy 1 association
===============================================================================
Security Policy
===============================================================================
Policy Id    : 1                                Applied        : Yes
Name         : Inbound Policy
Scope        : Template                         Def. Action    : Reject
Entries      : 1
Description  : common egress policy
-------------------------------------------------------------------------------
Policy Match Criteria : IP
-------------------------------------------------------------------------------
===============================================================================

===============================================================================
Associations
Zone-Id    Name                     Type        Svc-Id        Bypass
-------------------------------------------------------------------------------
1          Service Inbound Zone     IES         100           No
-------------------------------------------------------------------------------
Num of Associations: 1
===============================================================================
*A-ALU-1#

*A-ALU-1# show security policy 1 entry 1 detail
===============================================================================
Security Policy
===============================================================================
Policy Id    : 1                                Applied        : Yes
Name         : Inbound Policy
Scope        : Template                         Def. Action    : Reject
Entries      : 2
Description  : common egress policy
-------------------------------------------------------------------------------
Policy Match Criteria : IP
-------------------------------------------------------------------------------
Entry            : 1                                Active         : yes
Description      : match TCP and port
Match direction  : zone-inbound
Src. IP          : None                             Src. Port      : eq21
Dest. IP         : None                             Dest. Port     : None
Protocol         : tcp
ICMP Type        : Undefined                        ICMP Code      : Undefined
Profile ID       : DEFAULT                          Session        : Fwd-Dir-O*
Action           : nat                              Session Limit : None
Logging          : Suppressed
===============================================================================
*A-ALU-1#
```

Table 106 **Security Policy Field Descriptions (Detail)**

Label	Description
Policy Id	The security policy ID
Name	The name of the policy
Scope	Template — the policy is of type template
	Exclusive — the policy is of type exclusive
Entries	The number of entries configured in this policy ID
Description	The security policy description
Applied	No — the security policy ID has not been applied
	Yes — the security policy ID is applied
Def. Action	Reject — the default action for packets that do not match the policy entries is to reject
Policy Match Criteria	
Entry	The policy entry ID
Description	The policy entry description
Match Direction	Zone inbound — the match criteria is applied to packets inbound to the zone
	Zone outbound — the match criteria is applied to packets outbound from the zone
	Both — the match criteria is applied to packets both inbound to and outbound from the zone
Src. IP	The source IP address and prefix length match criterion
Dest. IP	The destination IP address and prefix length match criterion
Protocol	The protocol for the match criteria. Undefined indicates no protocol specified.
ICMP Type	The ICMP type match criterion. Undefined indicates no ICMP type is specified.
Profile ID	The profile ID
Active	No — the policy match criteria entry is not active
	Yes — the policy match criteria entry is active

Table 106 **Security Policy Field Descriptions (Detail) (Continued)**

Label	Description
Action	nat — applies NAT to the packets matching the profile entry
	reject — rejects packets matching the profile entry on the CSM session
	forwards — forward packets matching the profile entry
	drops — drop the packets matching the profile entry on the datapath session
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
Session	Indicates whether the security session is bidirectional or unidirectional (forward only)
Session Limit	The maximum number of concurrent sessions
Logging	Indicates whether logging has been enabled per policy entry or per zone, or whether all logs generated by the entry are suppressed

profile

Syntax **profile** [*profile-id* | *name*] [**detail**] [**association**]

Context show>security

Description This command displays security profile information.

Parameters *profile-id* — displays detailed information for the specified profile ID

Values 1 to 65535

name — displays information on the specified profile name

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

detail — displays detailed information on the specified profile ID

association — displays counter information for the specified profile ID

Output The following output is an example of security profile information, and Table 107 describes the fields.

Output Example

```
*A-ALU-1# show security profile 1 detail
===============================================================================
Security Profile
===============================================================================
Profile Id        : 1                                 Applied        : Yes
Name              : DEFAULT
Description       : Default Session Profile
Packet           :
  Fragmentation           : Allowed
Application               : Inspection-Disabled      ALG            : Auto
Timeouts          :
  TCP Syn-Rcvd    : strict 15 seconds
  TCP Transitory  : strict 4 min
  TCP Established : idle 2 hrs 4 min
  TCP Time-Wait   : None
  UDP Initial     : strict 15 seconds
  UDP Established : idle 5 min
  UDP DNS         : strict 15 seconds
  ICMP Request    : strict 1 min
  OTHER Sessions    : strict 10 min
===============================================================================
*A-ALU-1#
```

Table 107 **Security Profile Field Descriptions (Detail)**

Label	Description
Profile Id	The security profile ID
Name	The name of the profile
Description	The profile description
Packet	The configured packet level options
Fragmentation	Controls processing of IP packet fragments on a session
Application	The configured profile application parameters
TCP Syn-Rcvd	Timeout configured for a TCP session in a SYN state
TCP Transitory	Timeout configured for a TCP session in a transitory state
TCP Established	Timeout configured for a TCP session in an established state
TCP Time-Wait	Timeout configured for a TCP session in a time-wait state
UDP Initial	Timeout configured for a UDP session in an initial state
UDP Idle	Timeout configured for a UDP session in an idle state
UDP DNS	Timeout configured for a UDP session with destination port 53
ICMP Request	Timeout configured for an ICMP session in which an ICMP request is sent but no ICMP response is received

Table 107 **Security Profile Field Descriptions (Detail) (Continued)**

Label	Description
Other Sessions	Timeout for sessions other than TCP, UDP, or ICMP
Applied	No — the security profile ID has not been applied
	Yes — the security profile ID is applied
ALG	Application level gateway: auto, FTP, or TFTP

session-summary

Syntax **session-summary** [**service** *service-id*] [**router** *router-instance*]

Context show>security

Description This command displays a summary of active security sessions for zones.

Output The following output is an example of security session summary information, and Table 108 describes the fields.

Output Example

```
*A-ALU-1# show security session-summary
===============================================================================
Session Summary
===============================================================================
Total Created       : 7
Active              : 7                     Limit              :  16383
Utilization         :   0% (OK)
Hi-Wtr-Mark         : None                    Lo-Wtr-Mark         :  None
===============================================================================
===============================================================================
Zone Session Summary
===============================================================================
                                                              Inbound    Outbound
Zone-Id   Name                            Type    Svc-Id    Sessions   Sessions
-------------------------------------------------------------------------------
1         Service Inbound Zone            IES     100       4          3
2         Service Outbound Zone           IES     200       0          0
-------------------------------------------------------------------------------
Num of Zones: 2
===============================================================================
*A-ALU-1# show security session-summary service 100
===============================================================================
Session Summary
===============================================================================
Total Created       : 7
Active              : 7                     Limit              :  16383
Utilization         :   0% (OK)
Hi-Wtr-Mark         : None                    Lo-Wtr-Mark         :  None
===============================================================================
```

```
===============================================================================
Zone Session Summary
===============================================================================
                                                          Inbound    Outbound
Zone-Id   Name                            Type    Svc-Id  Sessions   Sessions
1         Service Inbound Zone            IES     100     4          3
-------------------------------------------------------------------------------
Num of Zones: 1
===============================================================================
*A-ALU-1# show security session-summary router 1
===============================================================================
Session Summary
===============================================================================
Total Created       : 7
Active              : 7                     Limit              :  16383
Utilization         :   0% (OK)
Hi-Wtr-Mark         : None                    Lo-Wtr-Mark        :  None
No Matching Zones
===============================================================================
Zone Session Summary
===============================================================================
                                                          Inbound    Outbound
Zone-Id   Name                            Type    Svc-Id  Sessions   Sessions
-------------------------------------------------------------------------------
===============================================================================
*A-ALU-1#
```

Table 108 Session Summary Field Descriptions

Label	Description
Total Created	The total number of security sessions created since node startup or last cleared statistics
Active	The number of security sessions that are currently active
Limit	The total number of security sessions allowed
Utilization	The number of active security sessions, expressed as a percentage of the total allowed
Hi-Wtr-Mark	Indicates the high-water mark threshold configured for security sessions
Lo-Wtr-Mark	Indicates the low-water mark threshold configured for security sessions
Zone-Id	The zone ID
Name	The name of the zone
Type	The zone type
Svc-Id	The service ID
Inbound Sessions	The number of sessions inbound to the zone

Table 108 **Session Summary Field Descriptions (Continued)**

Label	Description
Outbound Sessions	The number of sessions outbound from the zone

summary

Syntax **summary**

Context show>security

Description This command displays a summary of security information.

Output The following output is an example of security summary information.

Output Example

```
*A-ALU-1# show security summary
===============================================================================
Security
===============================================================================
Policy State     : Committed
Last Commit      : 05/07/2015 03:05:34
Policies         : 2
Profiles         : 2
Zones            : 2

Sessions
Active           : 5223                            Limit        : 16383
Utilization      : 85% (ALARM)
Hi-Wtr-Mark      : 80%                             Lo-Wtr-Mark  : 50%
===============================================================================
*A-ALU-1#
```

zone

Syntax **zone** [**service** *service-id*] [**router** *router-instance*]
zone [*zone-id* | *zone-name*] [**detail**]
zone [*zone-id* | *zone-name*] **interface**
zone [*zone-id* | *zone-name*] **statistics**

Context show>security

Description This command displays security zone information. During a CSM activity switch, security session statistics roll back to zero; however, statistics for active security sessions do not.

Parameters *service-id* — displays detailed information for the specified service ID

Values 1 to 2147483647

router-instance — displays detailed information for the specified router instance

Values 1 to 2147483647

zone-id — displays detailed information for the specified zone ID

Values 1 to 65534

zone-name — displays information for the specified name

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

detail — displays detailed information on the specified zone

interface — specifies the router interface

statistics — displays statistics for the specified zone ID

Output The following output is an example of zone information.

Output Example

```
*A:7705:Dut-A# show security zone 1 detail
===============================================================================
Security Zone
===============================================================================
Zone Id          : 1                                  State          : Committed
Name             : Service Inbound Zone
Description      : NAT on public
Type             : IES                                Service Id     : 100
Policy           : Inbound Policy                     Bypass         : No
Log              : SecurityLog11
Last Commit      : 10/22/2015 01:07:57
===============================================================================
===============================================================================
Interfaces
===============================================================================
Name                            IP-Address      Type    Bypass Filtering
-------------------------------------------------------------------------------
ies-100-10.30.10.1              10.30.10.1      IES     No     Active
-------------------------------------------------------------------------------
Num of Interfaces: 1
===============================================================================
===============================================================================
Zone Queue Statistics
===============================================================================
Rx Queue CTL                                    Packets                 Octets
  Forwarded :                                     24852                54632962
  Dropped   :                                         0                       0
===============================================================================
===============================================================================
Zone Policy Statistics
===============================================================================
                                                Inbound                Outbound
-------------------------------------------------------------------------------
Total Sessions Created                              4                       3
  Action: Forward                                   0                       0
          NAT                                       4                       3
          Drop                                      0                       0
```

```
Policy Discards
  Reject Action                                          0                     0
  No Rule Matched                                        0                 12400
===============================================================================
===============================================================================
Zone Active Session Summary
===============================================================================
                                                    Active                 Limit
-------------------------------------------------------------------------------
Inbound                                                  4
  TCP                                                    1                  None
  UDP                                                    2                  None
  ICMP                                                   1                  None
  Other                                                  0                  None
Outbound                                                 3
  TCP                                                    1                  None
  UDP                                                    2                  None
  ICMP                                                   0                  None
  Other                                                  0                  None
===============================================================================
*A:7705:Dut-A#

*A:7705:Dut-A# show security zone 1 statistics
===============================================================================
Zone Queue Statistics
===============================================================================
Rx Queue CTL                                       Packets                Octets
  Forwarded :                                        24732              54368782
  Dropped   :                                            0                     0
===============================================================================
===============================================================================
Zone Policy Statistics
===============================================================================
                                                   Inbound               Outbound
-------------------------------------------------------------------------------
Total Sessions Created                                   4                     3
  Action: Forward                                        0                     0
          NAT                                            4                     3
          Drop                                           0                     0

Policy Discards
  Reject Action                                          0                     0
  No Rule Matched                                        0                 12340
===============================================================================
===============================================================================
Zone Active Session Summary
===============================================================================
                                                    Active                 Limit
-------------------------------------------------------------------------------
Inbound                                                  4
  TCP                                                    1                  None
  UDP                                                    2                  None
  ICMP                                                   1                  None
  Other                                                  0                  None
Outbound                                                 3
  TCP                                                    1                  None
  UDP                                                    2                  None
  ICMP                                                   0                  None
  Other                                                  0                  None
```

```
===============================================================================
*A:7705:Dut-A#
```

nat pool

Syntax **nat pool** [*pool-id* | *pool-name*] [**detail**]

Context show>security>zone

Description This command displays NAT pool information.

Parameters *pool-id* — displays detailed information for the specified zone pool ID

Values 1 to 100

pool-name — displays information for the specified zone pool name

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

detail — displays detailed information on the specified pool ID

Output The following output is an example of zone pool information.

Output Example

```
*A-ALU-1# show security zone 1 nat pool 1 detail
===============================================================================
Security Zone
===============================================================================
Zone Id          : 1                                  State          : Committed
Name             : Service Inbound Zone
===============================================================================

===============================================================================
NAT Pool
===============================================================================
Pool Id          : 1                                Direction          : Inbound
Type             : source-nat
Name             : (Not Specified)
Description      : Pool 1:
-------------------------------------------------------------------------------
Entry Id         : 1                                Direction          : Inbound
IP Address       : ies-100-10.30.10.1                Port               : Any

-------------------------------------------------------------------------------
Num of Entries   : 1
===============================================================================
*A-ALU-1#
```

policy

Syntax **policy** [**entry** *entry-id*] [**detail**] [**statistics**]

Context show>security>zone

Description This command displays security zone policy information.

Parameters *entry-id* — displays detailed information for the specified entry ID

Values 1 to 65535

detail — displays detailed information on the zone policy

statistics — displays statistics for the zone policy

Output The following output is an example of zone policy information.

Output Example

```
*A-ALU-1# show security zone 1 policy statistics
===============================================================================
Security Zone
===============================================================================
Zone Id          : 1                                 State          : Committed
Name             : Service Inbound Zone
===============================================================================

===============================================================================
Policy
===============================================================================
Pool Id          : 1                                 Direction          : Inbound
Type             : source-nat
Name             : (Not Specified)
Description      : Pool 1:
-------------------------------------------------------------------------------
Entry            : 1                                 Active             : yes
Active Matches   : 1                                 Session Limit      : Any
Total Matches    : 1
Entry            : 2                                 Active             : yes
Active Matches   : 1                                 Session Limit      : None
Total Matches    : 1
-------------------------------------------------------------------------------
Num of Entries   : 2
===============================================================================
*A-ALU-1#
```

session

Syntax **session** [**inbound** | **outbound**] [**forward** | **nat**]
session [*session-id*] [**detail**]
session [*session-id*] [**statistics**]

Context show>security>zone

Description This command displays security zone session information.

The **detail** command shows detailed session information on the master node in a multi-chassis firewall configuration. The command does not show state, session, or time remaining information for the slave node.

Parameters *session-id* — displays detailed information for the specified session ID

Values 1 to 16383

inbound — displays zone inbound sessions

outbound — displays zone outbound sessions

forward — displays forwarded packets

nat — displays packets that have had NAT applied to them

detail — displays detailed information on the zone policy

statistics — displays statistics for the zone policy

Output The following output is an example of zone session information.

Output Example

```
*A-ALU-1# show security zone 1 session
===============================================================================
Security Zone
===============================================================================
Zone Id          : 1                                 State          : Committed
Name             : Service Inbound Zone
===============================================================================

===============================================================================
Inbound Sessions
===============================================================================
Sess-Id                    Source                  Outside NAT Mapping
Proto      Action From     Destination
-------------------------------------------------------------------------------
00000001    NAT            <Base> 10.100.0.2:161   -->10.30.10.1:5000
udp                        10.100.0.2:161
00000002    NAT            <Base> 10.100.0.2:21    -->10.30.10.1:5000
udp                        10.100.0.2:21
-------------------------------------------------------------------------------
Num of Sessions   : 2
===============================================================================

===============================================================================
Outbound Sessions
===============================================================================
Sess-Id                    Source                  Outside NAT Mapping
Proto      Action To       Destination
-------------------------------------------------------------------------------
No Outbound Sessions
===============================================================================
*A-ALU-1#
```

Output Example

```
*A-ALU-1# show security zone 1 session 1 statistics
===============================================================================
Security Zone
===============================================================================
Zone Id          : 1                                State          : Committed
Name             : Service Inbound Zone
===============================================================================

===============================================================================
Session 1 Traffic Statistics
===============================================================================
                           Forward                    Reverse
-------------------------------------------------------------------------------
Passed
  Packets                  2042929                    2042589
  Octets                   216550474                  224684790
===============================================================================
*A-ALU-1#
```

Output Example (Master in a Multi-Chassis Firewall)

```
A:7705:Dut-A# show security zone 1 session 6 detail
===============================================================================
Security Zone
===============================================================================
Zone Id          : 1                                State          : Committed
Name             : Service Inbound Zone
===============================================================================
===============================================================================
Security Session Details
===============================================================================
Session Id    : 6                        Action        : NAT
Created       : 04/11/2019 17:33:56
Protocol      : UDP                      ALG           : None
State         : UDP-ESTABLISHED          Session       : Active
Time Remaining: -

Source        :                          Destination   :
  Zone        : <BASE>                     Zone        : 1
  Ip-Address  : 10.100.0.2                 Ip-Address  : 30.100.0.2
  Port        : 3010                       Port        : 161

Session Profile
  Bidirection*: Yes
  CSM Inspect*: No
  Fwd Policer : None
  Rev Policer : None
  IP
    Fragments : Allowed
    Options   : Permit-Any
  ICMP Type 3 : Restrict
  Timeouts
    Init      : strict 15 sec
    Establish*: idle 5 min

-------------------------------------------------------------------------------
```

```
Session Security Trace
-------------------------------------------------------------------------------
[INGRESS] Base:ip-10.50.10.1
  [EGRESS] INBOUND-PLCY:1-2 Profile:10 Action:nat
  [ACTION] SRC-NAT:  10.100.0.2:3010 -> 10.30.60.1:5000
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:7705:Dut-A#
```

5.7.2.3 Clear Commands

ip

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

Context clear>filter

Description This command clears the counters associated with the IPv4 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 IPv4 filter policy entries

Parameters *ip-filter-id* — the IPv4 filter policy ID or filter name

Values 1 to 65535 or *filter-name* (up to 64 characters)

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

Values 1 to 64

ingress — only the ingress counters will be cleared

egress — only the egress counters will be cleared

ipv6

Syntax **ipv6** *ipv6-filter-id* [**entry** *entry-id*] [**ingress** | **egress**]

Context clear>filter

Description This command clears the counters associated with the IPv6 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 IPv6 filter policy entries

Parameters *ipv6-filter-id* — the IPv6 filter policy ID or filter name

Values 1 to 65535 or *filter-name* (up to 64 characters)

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

Values 1 to 64

ingress — only the ingress counters will be cleared

egress — only the egress counters will be cleared

log

Syntax **log** *log-id*

Context clear>filter

Description This command clears the entries associated with the specified filter log. The clear command applies only to logs whose destination is to memory.

Parameters *log-id* — the filter log ID destination expressed as a decimal integer

Values 101 to 199

mac

Syntax **mac** *mac-filter-id* [**entry** *entry-id*] [**ingress** | **egress**]

Context clear>filter

Description This command clears the counters associated with the MAC 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 MAC filter policy entries

Parameters *mac-filter-id* — the MAC filter policy ID or filter name

Values 1 to 65535 or *filter-name* (up to 64 characters)

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

Values 1 to 64

ingress — only the ingress counters will be cleared

egress — only the egress counters will be cleared (currently not supported on the 7705 SAR)

session

Syntax **session** [*session-id*] [**statistics**]

Context clear>security

Description This command clears the specified sessions and can also clear the associated session statistics.

Parameters *session-id* — clears the sessions associated with the specified session ID

Values 1 to 16383

statistics — clears statistics for the specified session ID

zone

Syntax **zone** [*zone-id* | *zone-name*]
zone [*zone-id* | *zone-name*] **sessions** [**inbound** | **outbound** | **all**]
zone [*zone-id* | *zone-name*] **statistics**

Context clear>security

Description This command clears security zone information.

Parameters *zone-id* — specifies the zone ID

Values 1 to 65534

zone-name — specifies the zone name

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

sessions — removes sessions associated with the specified zone ID

inbound — removes inbound sessions associated with the specified zone ID

outbound — removes outbound sessions associated with the specified zone ID

all — removes all sessions associated with the specified zone ID

statistics — clears statistics for the specified zone ID

5.7.2.4 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 IPv4 filter policy.

Parameters *ip-filter-id* — the IPv4 filter policy ID or filter name

Values 1 to 65535 or *filter-name* (up to 64 characters)

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

Values 1 to 64

seconds — configures the interval for each display in seconds

Values 3 to 60

Default 5

repeat — configures how many times the command is repeated

Values 1 to 999

Default 10

absolute — the raw statistics are displayed without processing. No calculations are performed on the delta or rate statistics.

rate — the rate per second for each statistic is displayed instead of the delta

filter

Syntax **filter ipv6** *ipv6-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor

Description This command monitors the counters associated with the IPv6 filter policy.

Parameters *ipv6-filter-id* — the IPv6 filter policy ID or filter name

Values 1 to 65535 or *filter-name* (up to 64 characters)

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

Values 1 to 64

seconds — configures the interval for each display in seconds

Values 3 to 60

Default 5

repeat — configures how many times the command is repeated

Values 1 to 999

Default 10

absolute — the raw statistics are displayed without processing. No calculations are performed on the delta or rate statistics.

rate — the rate per second for each statistic is displayed instead of the delta

filter

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

Context monitor

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

Parameters *mac-filter-id* — the MAC filter policy ID or filter name

Values 1 to 65535 or *filter-name* (up to 64 characters)

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

Values 1 to 64

seconds — configures the interval for each display in seconds

Values 3 to 60

Default 5

repeat — configures how many times the command is repeated

Values 1 to 999

Default 10

absolute — the raw statistics are displayed without processing. No calculations are performed on the delta or rate statistics.

rate — the rate per second for each statistic is displayed instead of the delta

6 Cflowd

This chapter provides information about filter policies and management.

Topics in this chapter include:

6.1 Cflowd Overview

Cflowd is a tool used to sample IPv4, IPv6, MPLS, and Ethernet traffic data flows through a router. Cflowd enables traffic sampling and analysis by ISPs and network engineers to support capacity planning, trends analysis, and characterization of workloads in a network service provider environment.

Cflowd is also useful for traffic engineering, network planning and analysis, network monitoring, developing user profiles, data warehousing and mining, as well as security-related investigations. Collected information can be viewed in port, AS, or network matrices and pure flow structures. The amount of data stored depends on the Cflowd configurations.

Cflowd maintains a list of data flows through a router. A flow is a unidirectional traffic stream defined by several characteristics such as source and destination IP addresses, source and destination ports, inbound interface, IP protocol, and type of service (ToS) bits.

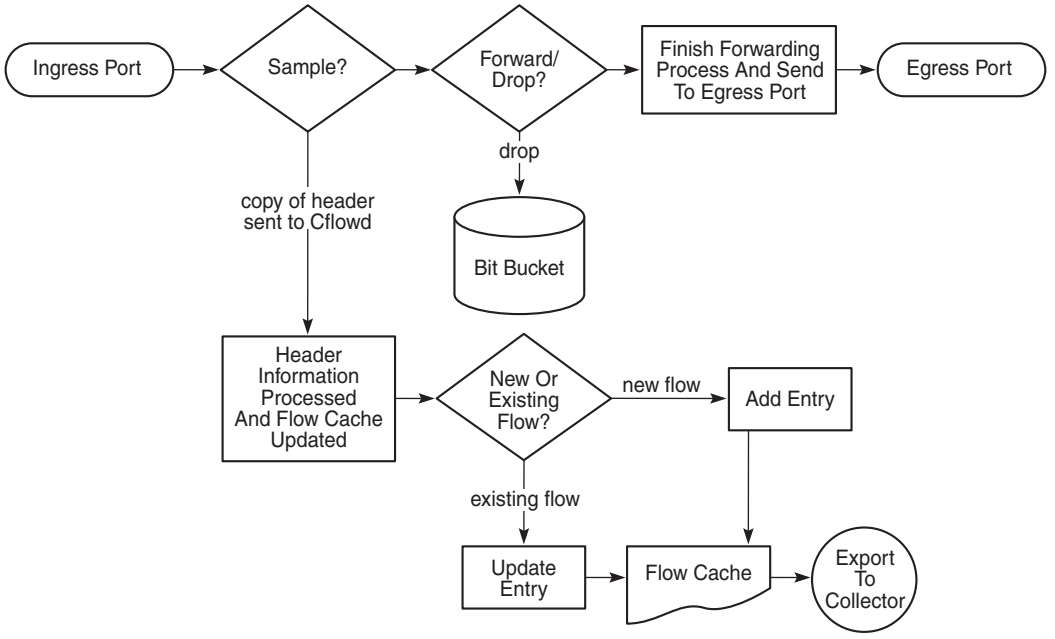
When a router receives a packet that is sampled by Cflowd, and for which it currently does not have a flow entry, a flow structure is initialized to maintain state information regarding that flow, such as the number of bytes exchanged, IP addresses, port numbers, and AS numbers. Each subsequent packet that is sampled and that matches the parameters of the flow contributes to the byte and packet count of the flow until the flow is terminated and exported to a collector for storage.

The 7705 SAR supports Cflowd version 9 and 10 on Ethernet ports on all cards except the 8-port Ethernet Adapter card. On the 2-port 10GigE (Ethernet) Adapter card and 2-port 10GigE (Ethernet) module, only the virtual port supports sampling. If Cflowd is configured on an IP interface or Layer 2 SAP that is associated with a LAG group with one or more member ports on an 8-port Ethernet Adapter card, no packets are sampled from those ports.

6.1.1 Operation

Figure 15 shows the basic operation of the Cflowd feature. This flow example is only used to describe the basic steps that are performed. It is not intended to specify how Cflowd is implemented.

Figure 15 **Basic Cflowd Operation**



The basic Cflowd steps are as follows.

1. As a packet ingresses a port, a decision is made to forward or drop the packet.
2. A decision is then made as to whether the packet should be sampled; if so, the forward/drop status is appended to the header information for processing by Cflowd.
3. If a new flow is found, a new entry is added to the cache. If the flow already exists in the cache, the flow statistics are updated.
4. If a new flow is found and the maximum number of entries are already in the flow cache, the earliest expiry entry is terminated. The earliest expiry entry is the next flow that will expire due to the active or inactive timer expiration.
5. If a flow has been inactive for a period of time equal to, or greater than, the inactive timer (default 15 s), the entry is terminated.
6. If a flow has been active for a period of time equal to, or greater than, the active timer (default 30 min), the entry is terminated.

The sample rate and cache size are configurable values. The sample rate default is 1000 with a range of one to 1 000 000. The cache size default is 65 536 flow entries with a range of 1000 to 250 000.

A flow terminates when one of the following conditions is met:

- the inactive timer expires

  A flow is terminated when no packets are seen for the flow for a number of seconds equal to, or greater than, the inactive timer. The default inactive timeout period is 15 s, with a range of 10 to 600 s.
- the active timer expires

  A flow is terminated if it has been active for a period of time equal to, or greater than, the active timer, even if there are packets coming in for the flow. The default active timeout period is 30 min, with a range of 1 to 600 min.
- the user executes a **clear cflowd** command
- any other measure is met that applies to aggressively age flows as the cache becomes too full (such as overflow percent)

When a flow is terminated, the collected data is formatted and exported from the cache to an external collector that maintains an accumulation of historical data flows that network operators can use to analyze traffic patterns. Flow data is exported in one of the following formats:

- version 9 — generates a variable export record, depending on user configuration and sampled traffic type (IPv4, IPv6, or MPLS) for each individual flow captured. Version 9 is interoperable with RFC 3954, *Cisco Systems NetFlow Services Export Version 9*.
- version 10 (IPFIX) — generates a variable export record, depending on user configuration and sampled traffic type (IPv4, IPv6, MPLS, or Ethernet Layer 2) for each individual flow captured. Version 10 is interoperable with RFC 5101 and 5102 from the IETF as the IP Flow Information Export (IPFIX) standard.

6.1.2 Sampling

To avoid stressing router processors with excessive sampling, Cflowd is not required to examine every packet received by the router. The sampling rate can be configured to be every packet or up to every 1 000 000 packets, with a default rate of 1000 packets. A larger rate value provides more flexibility to avoid congestion on smaller platforms. Sampling at too high a rate over an extended period of time can burden router processing resources. Sampling is supported in ingress and egress directions for Layer 3 services. For Layer 2 services, only ingress sampling is supported.

The following data is maintained for each individual flow in the raw flow cache:

- source IP address
- destination IP address

- source port
- destination port
- forwarding status
- input interface
- output interface
- IP protocol
- TCP flags
- first timestamp (of the first packet in the flow)
- last timestamp (timestamp of last packet in the flow prior to expiry of the flow)
- source AS number for peer and origin (taken from BGP)
- destination AS number for peer and origin (taken from BGP)
- IP next hop
- BGP next hop
- ICMP type and code
- IP version
- source prefix (from routing)
- destination prefix (from routing)
- MPLS label stack from label 1 to 6

Within the raw flow cache, the following characteristics are used to identify an individual flow:

- ingress interface
- source IP address
- destination IP address
- source transport port number
- destination transport port number
- IP protocol type
- IP ToS byte
- forwarding status
- virtual router ID
- ICMP type and code
- direction
- MPLS labels

6.1.3 Collectors

A collector defines how data flows should be exported from the flow cache. A maximum of five collectors can be configured and at least one must be configured for Cflowd to be active. Each collector is identified by a unique IP address and UDP port value. Each collector can only export traffic in one version type: version 9 or version 10.

The parameters within a collector configuration can be modified.

6.1.4 Templates

Flow data is sent to the designated collector using a predefined template. The template used is based on the type of flow for which the data was collected (IPv4, IPv6, MPLS, or Ethernet Layer 2) and the configuration of the **template-set** parameter. Table 109 lists these values and the corresponding template used to export the flow data.

Table 109 **Cflowd Templates**

Traffic Flow	Template Set		
	basic	**mpls-ip**	**l2-ip**
IPv4	Basic IPv4	MPLS-IPv4	—
IPv6	Basic IPv6	MPLS-IPv6	—
MPLS	Basic MPLS	MPLS-IP	—
Ethernet [1]	—	—	L2-IP

Note:

1. Only supported on collectors configured for version 10 format.

Each flow exported to a collector configured for either the version 9 or version 10 format is sent using one of the templates listed in Table 109.

Table 110 to Table 114 list the fields in each template listed in Table 109.

Table 110 **Basic IPv4 Template**

Field Name	Field ID
IPv4 Src Addr	8
IPv4 Dest Addr	12
IPv4 Nexthop	15
BGP Nexthop	18
Ingress Interface	10
Egress Interface	14
Packet Count	2
Byte Count	1
Start Time	22
End Time	21
Flow Start Milliseconds [1]	152
Flow End Milliseconds [1]	153
Src Port	7
Dest Port	11
Forwarding Status	89
TCP control Bits (Flags)	6
IPv4 Protocol	4
IPv4 TOS	5
IP version	60
ICMP Type & Code	32
Direction	61
BGP Source ASN	16
BGP Dest ASN	17
Source IPv4 Prefix Length	9
Dest IPv4 Prefix Length	13
Minimum IP Total Length	25
Maximum IP Total Length	26

Table 110 **Basic IPv4 Template (Continued)**

Field Name	Field ID
Minimum TTL	52
Maximum TTL	53
Multicast Replication Factor	99
IsMulticast [1]	206
Ingress VRFID [1]	234
Egress VRFID [1]	235

Note:

1. Only sent to collectors configured for version 10 format.

Table 111 **Basic IPv6 Template**

Field Name	Field ID
IPv6 Src Addr	27
IPv6 Dest Addr	18
IPv6 Nexthop	62
IPv6 BGP Nexthop	63
IPv4 Nexthop	15
IPv4 BGP Nexthop	18
Ingress Interface	10
Egress Interface	14
Packet Count	2
Byte Count	1
Start Time	22
End Time	21
Flow Start Milliseconds [1]	152
Flow End Milliseconds [1]	153
Src Port	7
Dest Port	11

Table 111 **Basic IPv6 Template (Continued)**

Field Name	Field ID
Forwarding Status	89
TCP control Bits (Flags)	6
Protocol	4
IPv6 Extension Hdr	64
IPv6 Next Header [1]	193
IPv6 Flow Label	31
TOS	5
IP version	60
IPv6 ICMP Type & Code [1]	139
Direction	61
BGP Source ASN	16
BGP Dest ASN	17
IPv6 Src Mask	29
IPv6 Dest Mask	30
Minimum IP Total Length	25
Maximum IP Total Length	26
Minimum TTL	52
Maximum TTL	53
Multicast Replication Factor	99
IsMulticast [1]	206
Ingress VRFID [1]	234
Egress VRFID [1]	235

Note:

1. Only sent to collectors configured for version 10 format.

Table 112 **MPLS-IPv4 Template**

Field Name	Field ID
IPv4 Src Addr	8
IPv4 Dest Addr	12
IPv4 Nexthop	15
BGP Nexthop	18
Ingress Interface	10
Egress Interface	14
Packet Count	2
Byte Count	1
Start Time	22
End Time	21
Flow Start Milliseconds [1]	152
Flow End Milliseconds [1]	153
Src Port	7
Dest Port	11
Forwarding Status	89
TCP control Bits (Flags)	6
IPv4 Protocol	4
IPv4 TOS	5
IP version	60
ICMP Type & Code	32
Direction	61
BGP Source ASN	16
BGP Dest ASN	17
Source IPv4 Prefix Length	9
Dest IPv4 Prefix Length	13
MPLS Label 1	70
MPLS Label 2	71

Table 112 **MPLS-IPv4 Template (Continued)**

Field Name	Field ID
MPLS Label 3	72
MPLS Label 4	73
MPLS Label 5	74
MPLS Label 6	75
Minimum IP Total Length	25
Maximum IP Total Length	26
Minimum TTL	52
Maximum TTL	53
Multicast Replication Factor	99
IsMulticast [1]	206
Ingress VRFID [1]	234
Egress VRFID [1]	235

Note:

1. Only sent to collectors configured for version 10 format.

Table 113 **MPLS-IPv6 Template**

Field Name	Field ID
IPv6 Src Addr	27
IPv6 Dest Addr	28
IPv6 Nexthop	62
IPv6 BGP Nexthop	63
IPv4 Nexthop	15
IPv4 BGP Nexthop	18
Ingress Interface	10
Egress Interface	14
Packet Count	2
Byte Count	1

Table 113 **MPLS-IPv6 Template (Continued)**

Field Name	Field ID
Start Time	22
End Time	21
Flow Start Milliseconds [1]	152
Flow End Milliseconds [1]	153
Src Port	7
Dest Port	11
Forwarding Status	89
TCP control Bits (Flags)	6
Protocol	4
IPv6 Extension Hdr	64
IPv6 Next Header	193
IPv6 Flow Label	31
TOS	5
IP version	60
IPv4 ICMP Type & Code [2]	32
IPv6 ICMP Type & Code [1]	139
Direction	61
BGP Source ASN	16
BGP Dest ASN	17
IPv6 Src Mask	29
IPv6 Dest Mask	30
MPLS Label 1	70
MPLS Label 2	71
MPLS Label 3	72
MPLS Label 4	73
MPLS Label 5	74
MPLS Label 6	75

Table 113 **MPLS-IPv6 Template (Continued)**

Field Name	Field ID
Minimum IP Total Length	25
Maximum IP Total Length	26
Minimum TTL	52
Maximum TTL	53
Multicast Replication Factor	99
IsMulticast [1]	206
Ingress VRFID [1]	234
Egress VRFID [1]	235

Notes:

1. Only sent to collectors configured for version 10 format.
2. Only sent to collectors configured for version 9 format.

Table 114 **L2-IP (Ethernet) Flow Template for Version 10 Only**

Field Name [1]	Field ID
MAC Src Addr	56
MAC Dest Addr	80
Ingress Physical Interface	252
Egress Physical Interface [2]	253
Dot1q VLAN ID	243
Dot1q Customer VLAN ID	245
Post Dot1q VLAN ID	254
Post Dot1q Customer VLAN Id [3]	255
IPv4 Src Addr	8
IPv4 Dest Addr	12
IPv6 Src Addr	27
IPv6 Dest Addr	28
Packet Count	2

Table 114 **L2-IP (Ethernet) Flow Template for Version 10 Only (Continued)**

Field Name [1]	Field ID
Byte Count	1
Flow Start Milliseconds	152
Flow End Milliseconds	153
Src Port	7
Dest Port	11
TCP control Bits (Flags)	6
Protocol	4
IPv6 Option Header	64
IPv6 Next Header	196
IPv6 Flow Label	31
TOS	5
IP Version	60
ICMP Type Code	32

Notes:

1. Only one L2-IP (Ethernet) flow template is supported and exported to IPFIX (V10) collectors.
2. For SAP-to-SDP services, this value is the SDP ID.
3. For SAP-to-SDP services, this value is the VC ID.

6.2 Cflowd Configuration Process Overview

The following components must be configured for Cflowd to be operational:

- Cflowd must be enabled globally
- at least one collector must be configured and enabled
- sampling must be enabled on an interface on a port or service

6.3 Configuring Cflowd with CLI

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

Topics in this section include:

- Basic Cflowd Configuration
- Common Configuration Tasks
- Cflowd Configuration Management Tasks

6.4 Basic Cflowd Configuration

In order for Cflowd to be operational and sampling traffic:

- Cflowd must be enabled
- at least one collector must be configured and enabled
- sampling must be enabled on an interface applied to a port

The following example shows a Cflowd configuration:

```
A:NOK-1>config>cflowd# info detail
----------------------------------------------
     active-timeout 30
     cache-size 65536
     inactive-timeout 15
     overflow 1
     rate 1000
     collector 10.10.10.103:2055 version 9
          autonomous-system-type origin
          description "V9 collector"
          no shutdown
     exit
     template-retransmit 330
     exit
     no shutdown
----------------------------------------------
A:NOK-1>config>cflowd#
```

6.5 Common Configuration Tasks

This section provides a brief overview of the following common configuration tasks that must be performed to configure Cflowd:

- Enabling Cflowd
- Configuring Global Cflowd Parameters
- Configuring Cflowd Collector Parameters
- Specifying Cflowd Options on an IP Interface

6.5.1 Enabling Cflowd

Cflowd is disabled by default. Use the following CLI syntax to enable Cflowd:

CLI Syntax:
```
config# cflowd
no shutdown
```

The following example shows the default values when Cflowd is initially enabled. No collectors or collector options are configured.

```
A:NOK-1>config# info detail
...
#------------------------------------------
echo "Cflowd Configuration"
#------------------------------------------
    cflowd
        active-timeout 30
        cache-size 65536
        inactive-timeout 15
        overflow 1
        rate 1000
        template-retransmit 600
        no use-vtr-if-index
        no shutdown
    exit
#------------------------------------------
A:NOK-1>config#
```

6.5.1.1 Enabling Cflowd On a SAP

Use the following CLI syntax to enable Cflowd on a VPLS or Epipe SAP:

CLI Syntax:
```
config>service>vpls>sap# cflowd
no shutdown
```

CLI Syntax:
```
config>service>epipe>sap# cflowd
no shutdown
```

When Cflowd is configured on a SAP, all packets received are subject to analysis according to the global Cflowd configuration and exported according to the collector configurations.

The following example shows the default values when Cflowd is initially enabled on a VPLS SAP. The same defaults apply to Cflowd configured on an Epipe SAP.

```
*A:7705:Dut-A>config>service>vpls$ info
----------------------------------------------
            stp
                shutdown
            exit
            sap 1/1/1 create
                cflowd
                no shutdown
            exit
            sap 1/1/2 create
                cflowd
                no shutdown
            exit
            no shutdown
----------------------------------------------
```

6.5.2 Configuring Global Cflowd Parameters

The following common attributes apply to all instances of Cflowd:

- active timeout — controls the maximum time a flow record can be active before it will be automatically exported to the configured collectors
- inactive timeout — controls the minimum time before a flow is declared inactive. If the inactive timer expires and no new traffic is sampled for a flow, the flow is declared inactive and marked to be exported to the configured collectors
- cache size — defines the maximum size of the flow cache
- export mode — controls how exports are generated by the Cflowd process

- overflow — defines the percentage of flow records that are exported to all collectors if the flow cache size is exceeded
- rate — defines the system-wide sampling rate for Cflowd
- template retransmit— defines the interval (in seconds) before the version 9 and version 10 templates are retransmitted to all matching collectors

Use the following CLI commands to configure Cflowd parameters:

CLI Syntax:
```
config>cflowd#
active-timeout minutes
cache-size num-entries
export-mode {automatic | manual}
inactive-timeout seconds
overflow percent
rate sample-rate
template-retransmit seconds
no shutdown
```

The following example shows a global Cflowd configuration:

```
A:NOK-1>config>cflowd# info
#----------------------------------------
        active-timeout 20
        inactive-timeout 10
        overflow 10
        rate 100
#----------------------------------------
A:NOK-1>config>cflowd#
```

6.5.3 Configuring Cflowd Collector Parameters

To configure Cflowd collector parameters, enter the following commands:

CLI Syntax:
```
config>cflowd#
collector ip-address[:port] [version version]
   description description-string
   no shutdown
   template-set {basic | mpls-ip | l2-ip}
```

If a specific collector UDP port is not identified, flows are sent to port 2055 by default.

The following example shows a basic configuration for Cflowd collectors:

```
A:NOK-1>config>cflowd# info
----------------------------------------
        active-timeout 20
        inactive-timeout 10
```

```
        overflow 10
        rate 100
        collector 10.10.10.1:2000 version 9
            description "v9collector"
           template-set mpls-ip
        exit
        collector 10.10.10.2:5000 version 9
            description "Neighbor collector"
        exit
----------------------------------------
A:NOK-1>config>cflowd#
```

6.5.4 Specifying Cflowd Options on an IP Interface

When Cflowd is enabled on an interface, all packets received or transmitted are subject to analysis according to the global Cflowd configuration and exported according to the collector configurations.

The following must be configured to enable traffic sampling on the interface or SAP:

- Cflowd must be enabled
- at least one Cflowd collector must be configured and enabled
- Cflowd sampling parameters must be configured in the **config>router>interface** or **config>service>ies/vprn>interface** context.

The **interface** option must be selected to enable traffic sampling on an interface. If Cflowd is not enabled, traffic sampling will not occur on the interface.

6.5.4.1 Interface Configurations

CLI Syntax:

```
config>router>if# cflowd-parameters sampling
{unicast | multicast} type {interface} [direction
 {ingress-only | egress-only | both}]
no sampling {unicast | multicast}
```

When enabled on a router interface, Cflowd extracts traffic flow samples from the interface for analysis. Sampling is supported in the ingress and/or egress direction.

6.5.4.2 Service Interfaces

When enabled on a service interface, Cflowd collects routed traffic flow samples through the router for analysis. Cflowd is supported on IES and VPRN service interfaces. Sampling is supported in the ingress and/or egress direction.

The following command is used to configure Cflowd parameters on an IES interface and the same syntax is used for the VPRN context.

CLI Syntax:

```
config>service>ies>interface# cflowd-parameters sampling
  {unicast | multicast} type {interface} [direction
  {ingress-only | egress-only | both}]
no sampling {unicast | multicast}
```

6.6 Cflowd Configuration Management Tasks

This section provides a brief overview of the following Cflowd configuration management tasks:

- Modifying Global Cflowd Parameters
- Modifying Cflowd Collector Parameters

6.6.1 Modifying Global Cflowd Parameters

Cflowd parameter modifications apply to all instances where Cflowd is enabled. Changes are applied immediately. Use the following commands to modify global Cflowd parameters:

CLI Syntax:

```
config>cflowd#
active-timeout minutes
no active-timeout
cache-size num-entries
no cache-size
export-mode {automatic | manual}
inactive-timeout seconds
no inactive-timeout
overflow percent
no overflow
rate sample-rate
no rate
[no] shutdown
template-retransmit seconds
no template-retransmit
[no] use-vrtr-if-index
```

The following example shows the Cflowd command syntax to modify configuration parameters:

Example:

```
config>cflowd# active-timeout 60
config>cflowd# no inactive-timeout
config>cflowd# overflow 2
config>cflowd# rate 10
```

The following example shows the modified Cflowd configuration:

```
A:NOK-1>config>cflowd# info
#------------------------------------------
        active-timeout 60
        overflow 2
        rate 10
#------------------------------------------
A:NOK-1>config>cflowd#
```

6.6.2 Modifying Cflowd Collector Parameters

Use the following commands to modify Cflowd collector parameters:

CLI Syntax:

```
config>cflowd#
collector ip-address[:port] [version version]
no collector ip-address[:port]
   [no] description description-string
   [no] shutdown
   template-set {basic | mpls-ip | l2-ip}
```

The following example displays Cflowd modifications:

```
A:NOK-1>config>cflowd# info
----------------------------------------
        active-timeout 60
        overflow 2
        rate 10
        collector 10.10.10.1:2000 version 9
            description "AS info collector"
        exit
        collector 10.10.10.2:5000 version 9
            description "Test collector"
        exit
----------------------------------------
A:NOK-1>config>cflowd#
```

6.7 Cflowd Command Reference

6.7.1 Command Hierarchies

- Configuration Commands
- Show Commands
- Tools Commands (refer to Tools section of the 7705 SAR OAM and Diagnostics Guide)
- Clear Commands

6.7.1.1 Configuration Commands

config
- — [**no**] **cflowd**
  - — **active-timeout** *minutes*
  - — **no active-timeout**
  - — **cache-size** *num-entries*
  - — **no cache-size**
  - — **collector** *ip-address*[**:***port*] [**version** *version*]
  - — **no collector** *ip-address*[**:***port*]
    - — **description** *description-string*
    - — **no description**
    - — [**no**] **shutdown**
    - — **template-set** {**basic** | **mpls-ip** | **l2-ip**}
  - — **export-mode** {**automatic** | **manual**}
  - — **inactive-timeout** *seconds*
  - — **no inactive-timeout**
  - — **overflow** *percent*
  - — **no overflow**
  - — **rate** *sample-rate*
  - — **no rate**
  - — [**no**] **shutdown**
  - — **template-retransmit** *seconds*
  - — **no template-retransmit**
  - — [**no**] **use-vrtr-if-index**

6.7.1.2 Show Commands

show
- — **cflowd**
  - — **collector** [*ip-address*[**:***port*]] [**detail**]
  - — **interface** [*ip-int-name*]
  - — **l2-services**
  - — **status**

6.7.1.3 Clear Commands

clear
- — **cflowd**

6.7.2 Command Descriptions

6.7.2.1 Generic Commands

description

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

Context config>cflowd>collector

Description This command creates a text description stored in the configuration file for a configuration context.

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

Default no description

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

Context config>cflowd
config>cflowd>collector

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

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

The **no** form of this command administratively enables the entity.

Unlike other commands and parameters where the default state is not indicated in the configuration file, the **shutdown** and **no shutdown** states are always indicated in system-generated configuration files.

Default no shutdown

6.7.2.2 Configuration Commands

cflowd

Syntax [**no**] **cflowd**

Context config

Description This command enables the context to configure Cflowd.

The **no** form of this command removes all configuration under the **cflowd** context. This command can only be executed if Cflowd is in a shutdown state.

Default no cflowd

active-timeout

Syntax **active-timeout** *minutes*
no active-timeout

Context config>cflowd

Description This command configures the maximum amount of time before an active flow is aged out of the Cflowd cache. If an individual flow is active for this amount of time, the flow is aged out and exported. A new flow is created on the next packet sampled for that flow.

If the **active-timeout** value is changed while Cflowd is active, existing flows do not inherit the new value. The **active-timeout** value for a flow is set when the flow is first created in the Cflowd cache table and does not change dynamically.

The **no** form of this command resets the active timeout to the default value.

Default active-timeout 30

Parameters *minutes* — the amount of time before an active flow is aged out and exported

Values 1 to 600

cache-size

Syntax **cache-size** *num-entries*
no cache-size

Context config>cflowd

Description This command specifies the maximum number of active flows to maintain in the flow cache table.

The **no** form of this command resets the number of active entries to the default value.

Default cache-size 65536

Parameters *num-entries* — specifies the maximum number of entries maintained in the Cflowd cache

Values 1000 to 250000

collector

Syntax **collector** *ip-address*[:*port*] [**version** *version*]
no collector *ip-address*[:*port*]

Context config>cflowd

Description This command defines a flow data collector for Cflowd data. The IP address of the flow collector must be specified. The UDP port number is an optional parameter, but if it is not set, the default of 2055 is used for all collector versions. The version must be specified when a collector is first configured. To connect to a version 10 (IPFIX) collector using the IPFIX default port, specify port 4739 when configuring the collector. A maximum of five collectors can be configured.

The **no** form of this command removes the flow collector definition from the configuration and stops the export of data to the collector. The collector must be shut down to be deleted.

Default No Cflowd collector is configured by default.

Parameters *ip-address* — specifies the address of a remote Cflowd collector host to receive the exported Cflowd data

Values

ipv4-address	a.b.c.d
ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

port — specifies the UDP port number on the remote Cflowd collector host to receive the exported Cflowd data

Values 1 to 65535

Default 2055

version — specifies the version of the flow data collector and is required to initially configure the collector

Values 9 or 10

template-set

Syntax **template-set** {**basic** | **mpls-ip** | **l2-ip**}

Context config>cflowd>collector

Description This command specifies the set of templates sent to the collector when using Cflowd version 9 or version 10. The Layer 2 (Ethernet) template (**l2-ip** keyword) is only applicable for collectors using Cflowd version 10 and is only used for flows sampled on Epipe or VPLS services

Default template-set basic

Parameters **basic** — specifies that basic flow data is sent

mpls-ip — specifies that extended flow data is sent that includes IP and MPLS flow information

l2-ip — specifies that extended flow data is sent that includes Layer 2 (Ethernet) and IP flow information.

export-mode

Syntax **export-mode** {**automatic** | **manual**}

Context config>cflowd

Description This command controls how exports are generated by the Cflowd process. The default behavior is for flow data to be exported automatically based on the active and inactive timeout values. If manual mode is used, case flow data is only exported when the **tools>perform>cflowd>manual-export** command is issued. The only exception is if the Cflowd cache overflows, in which case, the automatic export process is used.

Default export-mode automatic

Parameters **automatic** — Cflowd flow data is automatically generated

manual — Cflowd flow data is exported only when manually triggered

inactive-timeout

Syntax **inactive-timeout** *seconds*
no inactive-timeout

Context config>cflowd

Description This command specifies the amount of time, in seconds, that must elapse without a packet matching a flow in order for the flow to be considered inactive.

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

If the **inactive-timeout** value is changed while Cflowd is active, existing flows do not inherit the new value. The **inactive-timeout** value for a flow is set when the flow is first created in the active cache table and does not change dynamically.

Default inactive-timeout 15

Parameters *seconds* — the amount of time, that must elapse without a packet matching a flow in order for the flow to be considered inactive

Values 10 to 600

overflow

Syntax **overflow** *percent*
no overflow

Context config>cflowd

Description This command specifies the percentage of the flow cache entries removed when the maximum number of entries is exceeded. The entries removed are the entries that have not been updated for the longest amount of time.

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

Default overflow 1

Parameters *percent* — specifies the percentage of the flow cache entries removed when the maximum number of entries is exceeded

Values 1 to 50

rate

Syntax **rate** *sample-rate*
no rate

Context config>cflowd

Description This command specifies the rate (N) at which traffic is sampled and sent for flow analysis. A packet is sampled every N packets; for example, when **sample-rate** is configured as 1, all packets are sent to the cache. When **sample-rate** is configured as 100, every 100th packet is sent to the cache.

The **no** form of this command resets the sample rate to the default value.

Default rate 1000

Parameters *sample-rate* — specifies the rate at which traffic is sampled

Values 1 to 1 000 000

template-retransmit

Syntax **template-retransmit** *seconds*
no template-retransmit

Context config>cflowd

Description This command specifies the interval at which template definitions are sent to the collector.

Default template-retransmit 600

Parameters *seconds* — specifies the interval between the sending of template definitions

Values 10 to 600

use-vrtr-if-index

Syntax [**no**] **use-vrtr-if-index**

Context config>cflowd

Description This command is used to export flow data using interface indexes (ifindex values), which can be used directly as the index into the IF-MIB tables for retrieving interface statistics. If this command is enabled, the ingressInterface (ID=10) and egressInterface (ID= 14) fields in IP flow templates used to export the flow data to Cflowd version 9 and version 10 collectors will be populated with the IF-MIB ifindex of that interface. In addition, for version 10 templates, two fields are available in the IP flow templates to specify the virtual router ID associated with the ingress and egress interfaces.

The **no** form of this command causes Cflowd to return to the default behavior of populating the ingress and egress interface IDs with the global interface index IDs.

Default no use-vrtr-if-index

6.7.2.3 Show Commands

The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

collector

Syntax **collector** [*ip-addr*[**:***port*]] [**detail**]

Context show>cflowd

Description This command displays the administrative and operational status of data collectors.

Parameters *ip-addr* — displays information only about the collector with the specified IP address

Default all collectors

:*port* — displays information only about the collector with the specified UDP port

Default all UDP ports

Values 1 to 65535

detail — displays details about all collectors or the specified collector

Output The following outputs are examples of Cflowd collector information:

- Cflowd collector output (Output Example, Table 115)
- Cflowd collector detail output (Output Example, Table 116)

Output Example

```
A:NOK1# show cflowd collector
===============================================================================
Cflowd Collectors
Legend: P - Packets, R - Records
===============================================================================
Host Address                    Port  Ver AS Type Admin Oper           Sent
-------------------------------------------------------------------------------
100.120.214.103                 2055  v9    -     up    up             0 P
138.120.214.224                 2055  v10   -     up    up           138 R
-------------------------------------------------------------------------------
Collectors : 2
===============================================================================
A:NOK1#
```

Table 115 **Cflowd Collector Field Descriptions**

Label	Description
Host Address	The IP address of a remote Cflowd collector host to receive the exported Cflowd data
Port	The UDP port number on the remote Cflowd collector host to receive the exported Cflowd data
Ver	The configured version for the associated collector
AS Type	The style of AS reporting used in the exported flow data. AS Type is not applicable to Cflowd version 9 or version 10.
Admin	The configured administrative state for this Cflowd remote collector host
Oper	The current operational status of this Cflowd remote collector host
Sent	The number of packets (P) or records (R) that have been transmitted to this remote collector host
Collectors	The total number of collectors using this IP address

Output Example

```
A:R51-CfmA# show cflowd collector detail
===============================================================================
Cflowd Collectors  (detail)
===============================================================================
Address                      : 138.120.135.103
Port                         : 2055
Description                  : Test v9 Collector
Version                      : 9
AS Type                      : -
Admin State                  : up
Oper State                   : up
Packets Sent                 : 1260
Last Changed                 : 03/03/2019 17:24:04
Last Pkt Sent                : 03/03/2019 18:07:10
Template set                 : Basic
-------------------------------------------------------------------------------
Traffic Type            Template Sent          Sent          Open       Errors
-------------------------------------------------------------------------------
IPv4              03/03/2019 18:06:29            51             1            0
MPLS                 No template sent             0             0            0
IPv6                 No template sent             0             0            0
===============================================================================
A:R51-CfmA#
```

Table 116 **Cflowd Collector Detailed Field Descriptions**

Label	Description
Address	The IP address of a remote Cflowd collector host to receive the exported Cflowd data
Port	The UDP port number on the remote Cflowd collector host to receive the exported Cflowd data
Description	A user-provided descriptive string for this Cflowd remote collector host.
Version	The version of the flow data sent to the collector
AS Type	The style of AS reporting used in the exported flow data. AS Type is not applicable to Cflowd version 9 or version 10.
Admin State	The configured administrative state for this Cflowd remote collector host
Oper State	The current operational status of this Cflowd remote collector host
Packets Sent	The number of packets sent to the collector
Records Sent	The number of Cflowd records that have been transmitted to this remote collector host
Last Changed	The time that this row entry was last changed
Last Pkt Sent	The time that the last Cflowd packet was sent to this remote collector host
Template Set	The type of Cflowd template
Traffic Type	The type of traffic flow that was sampled by Cflowd
Template Sent	The date and time that the Cflowd template was last sent
Sent	The number of packets with flow data sent to the associated collector
Open	The number of partially filled packets that have some flow data but are not yet filled or have been timed out (60 s maximum)
Errors	This counter increments when there was an error during exporting of the collector packet. The most common reason is a UDP unreachable destination for the configured collector.

interface

Syntax **interface** [*ip-int-name*]

Context show>cflowd

Description This command displays the administrative and operational status of the interfaces with Cflowd enabled.

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

Output The following output is an example of Cflowd interface information, and Table 117 describes the fields.

Output Example

```
*A:7705:Dut-A>config>router>if>cflowd# show cflowd interface "ip-1.20.1.3"
===============================================================================
Cflowd Interfaces
===============================================================================
Interface                       Router       IF Index    Type/Dir  Admin
  IPv4Address                                             Samp      Oper IPv4
  IPv6Address                                                       Oper IPv6
-------------------------------------------------------------------------------
ip-1.20.1.3                     Base         1           intf/ingr Up
  1.20.1.3/24                                             uni       Up
  ::114:103/120                                           uni       Up
ip-1.20.1.3                     Base         1           intf/ingr Up
  1.20.1.3/24                                             multi     Up
  ::114:103/120                                           multi     Up
-------------------------------------------------------------------------------
Interfaces : 2
===============================================================================
*A:7705:Dut-A>config>router>if>cflowd#
```

Table 117 **Cflowd Interface Field Descriptions**

Label	Description
Interface	The physical port identifier
IPv4 Address	The primary IPv4 address for the associated IP interface
IPv6 Address	The primary IPv6 address for the associated IP interface
Router	The virtual router index (Base = 1)
IF Index	The Global IP interface index
Type/Dir Samp	The Cflowd sampling type and direction
Admin	The administrative state of the interface

Table 117 **Cflowd Interface Field Descriptions (Continued)**

Label	Description
Oper IPv4	The operational state for IPv4 sampling
Oper IPv6	The operational state for IPv6 sampling

l2-services

Syntax **l2-services**

Context show>cflowd

Description This command displays information about the administrative and operational status of Cflowd on Layer 2 services.

Output The following output is an example of Cflowd status information, and Table 118 describes the fields.

Output Example

```
*A:7705:Dut-A# show cflowd l2-services
===============================================================================
Cflowd L2-Services
===============================================================================
ServiceId      Type        SAP                                    Admin  Oper
-------------------------------------------------------------------------------
10             Epipe       1/1/1:10                               Up     Up
20             Epipe       1/1/1:20                               Up     Up
1000           VPLS        1/1/1:1111                             Up     Up
-------------------------------------------------------------------------------
No. of SAPs: 3
===============================================================================
*A:7705:Dut-A#
```

Table 118 **Cflowd L2-services Field Descriptions**

Label	Description
ServiceID	The service identifier
Type	The service type
SAP	The SAP identifier
Admin	The administrative state of the Layer 2 service
Oper	The operational state of the Layer 2 service
No. of SAPs	The total number of SAPs

status

Syntax **status**

Context show>cflowd

Description This command displays information about the administrative and operational status of Cflowd.

Output The following output is an example of Cflowd status information, and Table 119 describes the fields.

Output Example

```
*A:7705:Dut-A>config>cflowd$ show cflowd status
===============================================================================
Cflowd Status
===============================================================================
Cflowd Admin Status  : Enabled
Cflowd Oper Status   : Disabled
Cflowd Export Mode   : Automatic
Active Timeout       : 30 minutes
Inactive Timeout     : 15 seconds
Template Retransmit  : 600 seconds
Cache Size           : 65536 entries
Overflow             : 1%
Sample Rate          : 1000
Aggregation Summary  : (Not Specified)
VRtr If Index Context: global
Active Flows         : 0
Dropped Flows        : 0
Total Pkts Rcvd      : 0
Total Pkts Dropped   : 0
Overflow Events      : 0
                                        Raw Flow Counts  Aggregate Flow Counts
Flows Created                                         0                       0
Flows Matched                                         0                       0
Flows Flushed                                         0                       0
===============================================================================
Version Info
===============================================================================
Version                      Status            Sent          Open        Errors
-------------------------------------------------------------------------------
     5                       Disabled             0             0             0
     8                       Disabled             0             0             0
     9                       Disabled             0             0             0
    10                       Disabled             0             0             0
===============================================================================
```

Table 119 **Cflowd Status Field Descriptions**

Label	Description
Cflowd Admin Status	The configured administrative state for this Cflowd remote collector host
Cflowd Oper Status	The current operational status of this Cflowd remote collector host
Cflowd Export Mode	Controls how exports are handled by the Cflowd process: Automatic or Manual
Active Timeout	The maximum amount of time, in minutes, before an active flow will be exported.
Inactive Timeout	The amount of time, that must elapse without a packet matching a flow in order for the flow to be considered inactive
Template Retransmit	The time in seconds before template definitions are sent
Cache Size	The maximum number of active flows to be maintained in the flow cache table
Overflow	The Percentage Of Flows To Be Flushed When The Flow Cache Size Has Been Exceeded
Sample Rate	The rate at which traffic is sampled and forwarded for Cflowd Analysis
Aggregation Summary	Not currently supported on the 7705 SAR
VRtr If Index Context	Indicates the ifindexes used to populate the flow records: “global” means that the flow records will be populated using the global interface IDs; “vrtr” means that the interface IDs from the IF-MIB will be used
Active Flows	The current number of active flows being collected
Dropped Flows	The total number of flows dropped due to cache overflow events
Total Pkts Rcvd	The total number of packets sampled and forwarded for Cflowd analysis
Total Pkts Dropped	The total number of Cflowd sample reports dropped due to cache overflow or processor overload
Overflow Events	The number of times the active cache overflowed
Flows Created	The number of times a flow was created; aggregated flow statistics are not currently supported on the 7705 SAR
Flows Matched	The number of times a packet was matched to a flow; aggregated flow statistics are not currently supported on the 7705 SAR

Table 119 **Cflowd Status Field Descriptions (Continued)**

Label	Description
Flows Flushed	The total number of flows that have been flushed from the system; aggregated flow statistics are not currently supported on the 7705 SAR
Version	The Cflowd version
Status	The status of the collector: Enabled or Disabled
Sent	The number of packets with flow data sent to the associated collector
Open	The number of partially filled packets that have some flow data but are not yet filled or have been timed out (60 s maximum)
Errors	This counter increments when there was an error during exporting of the collector packet. The most common reason is a UDP unreachable destination for the configured collector.

6.7.2.4 Clear Commands

cflowd

Syntax **cflowd**

Context clear

Description This command clears the raw flow caches that are sending flow data to the configured collectors. This action triggers all the flows to be discarded. The cache restarts flow data collection from a fresh state. This command also clears global statistics and collector statistics that are displayed using Cflowd **show** commands.

Default n/a

7 Route Policies

This chapter provides information about configuring route policies.

Topics in this chapter include:

7.1 Configuring Route Policies

This section contains information on the following topics:

- Routing Policy and MPLS
- Policy Statements
- Regular Expressions
- Community Expressions
- BGP and OSPF Route Policy Support
- When to Use Route Policies
- Troubleshooting the FIB

Route policies are used to manage the label database for MPLS and to control entries to the routing table for dynamic routing (see Routing Policy and MPLS).

For routing, the 7705 SAR supports two databases to store routes. The routing database (RIB) is composed of the routing information learned by the routing protocols, including static routes. The forwarding database (FIB) is composed of the routes actually used to forward traffic through a router. In addition, link-state databases are maintained by interior gateway protocols (IGPs) such as OSPF and IS-IS. Refer to the 7705 SAR Routing Protocols Guide for information on OSPF, IS-IS, and other routing protocols.

Routing protocols calculate the best route to each destination and place these routes in the forwarding table. The routes in the forwarding table are used to forward IP packets to neighbors.

As an example, operators can configure a routing policy that will not place routes associated with a specific origin in the routing table. These routes will not be used to forward data packets and these routes are not advertised by the routing protocol to neighbors.

Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Careful planning is essential to implement route policies that can affect the flow of routing information throughout the network. Before configuring and applying a route policy, operators should develop an overall plan and strategy to accomplish their intended routing actions.

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

7.1.1 Routing Policy and MPLS

Route policies can be used to manage the MPLS label database.

When used to manage the label database, route policies can be configured to determine which labels should be learned or advertised; for example, labels from a specified neighbor can be added to the label information base (LIB), while labels advertised by certain other neighbors can be discarded. Label learning of MPLS packets and, as a result, how the MPLS packets are forwarded, are based on the defined policies, if there are any. If no route policies are defined, all advertised labels received from neighbors are learned and placed in the LIB.

Refer to the “Label Distribution Protocol” section in the 7705 SAR MPLS Guide for more information on how routing policies can be used as LDP import or export policies to control the label bindings that an LSR accepts from, or advertises to, its peers.

7.1.2 Policy Statements

Route policies contain policy statements containing ordered entries that contain match conditions and actions that the user specifies. The entries should be sequenced from the most explicit to the least explicit. Packet forwarding and routing can be implemented according to defined policies. Policy-based routing allows the user to dictate where traffic can be routed, through specific paths, or whether to forward or drop the traffic. Route policies can match a given route policy entry and continue searching for other matches within either the same route policy or the next route policy.

The process can stop when the first complete match is found and the router executes the action defined in the entry, either to accept or reject packets that match the criteria or proceed to the next entry or the next policy. Matching criteria can be based on source, destination, or particular properties of a route. Route policies can be constructed to support multiple stages to the evaluation and setting various route attributes.

Other matching conditions can be provided by specifying criteria such as:

- autonomous system (AS) path policy options — a combination of AS numbers and regular expression operators
- community list — a group sharing a common property
- prefix list — a named list of prefixes
- to and from criteria — a route’s destination and source

7.1.2.1 Default Action Behavior

The default action of a policy applies to a route when the route does not match any of the entries of the policy. If a policy does not have any match entries, all routes are subject to the default action. If no default action is specified and the policy is the last one in a chain of policies, the default action is determined by the protocol that called the policy.

If a default action is defined for one or more of the configured route policies, the default action is handled as follows:

- The default action can be set to all available action states, including accept, reject, next-entry, and next-policy.
- If the action states accept or reject, the policy evaluation terminates and the appropriate result is returned.
- If a default action is defined and no matches occurred with the entries in the policy, the default action is used.
- If a default action is defined and one or more matches occurred with the entries of the policy, the default action is not used.

7.1.2.2 Denied IP Prefixes

The following IP address prefixes are not allowed by the routing protocols and the Route Table Manager and are not 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.

7.1.2.3 Controlling Route Flapping

Route flapping is defined as recurring changes of an advertised route between nodes. That is, the advertised route alternates (flaps) back and forth between two paths. This is typically caused by network problems that cause intermittent route failures. Route flap is defined in RFC 2439.

Route damping is a controlled acceptance of unstable routes from BGP peers so that any ripple effect caused by route flapping across BGP AS border routers is minimized. The rationale is to delay the use of unstable routes (flapping routes) to forward data and advertisements until the route stabilizes.

The Nokia implementation of route damping is based on the following parameters:

- Figure of Merit — a route is assigned a Figure of Merit (FoM), which is proportional to the frequency of flaps. The FoM algorithm can characterize a route's behavior over a period of time. See Damping for more information on FoM and damping.
- route flap — a route flap is not limited to the withdrawn route. It also applies to any change in the AS path or the next hop of a reachable route. A change in AS path or next hop indicates that the intermediate AS or the route-advertising peer is not suppressing flapping routes at the source or during the propagation. Even if the route is accepted as a stable route, the data packets destined for the route could experience unstable routing due to the unstable AS path or next hop.
- suppress threshold — when the configured suppress threshold is exceeded, the route is suppressed and not advertised to other peers. The state of the route is considered to be down from the perspective of the routing protocol.
- reuse threshold — when the FoM value falls below the configured reuse threshold and the route is still reachable, the route is advertised to other peers. The FoM value decays exponentially after a route is suppressed.

The two events that could trigger the route flapping algorithm are:

- route flapping — if a route flap is detected within a configured maximum route flap history time, the route's FoM is initialized and the route is marked as a potentially unstable route. Every time a route flaps, the FoM is increased and the route is suppressed if the FoM crosses the suppress threshold.
- route reuse timer trigger — a suppressed route's FoM decays exponentially. When it crosses the reuse threshold, the route is eligible for advertisement if it is still reachable.

If the route continues to flap, the FoM, with respect to time scale, looks like a sawtooth waveform with the exponential rise and decay of FoM. To control flapping, the following parameters can be configured:

- half-life — the half-life value is the time, expressed in minutes, required for a route to remain stable in order for one half of the FoM value to be reduced. For example, if the half-life value is 6 (min) and the route remains stable for 6 min, then the new FoM value is 3. After another 6 min passes and the route remains stable, the new FoM value is 1.5.
- max-suppress — the maximum suppression time, expressed in minutes, is the maximum amount of time that a route can remain suppressed
- suppress — if the FoM value exceeds the configured integer value, the route is suppressed for use or inclusion in advertisements
- reuse — if the FoM value falls below the configured reuse value, then the route can be reused

7.1.3 Regular Expressions

The ability to perform a filter match in the AS-PATH is supported. This feature allows customers to configure match criteria for specific sequences within the AS path so that they can be filtered out before cluttering the service provider's routing information base (RIB).

The 7705 SAR uses regular expression strings to specify match criteria for:

- an AS path string; for example, "100 200 300", where 100, 200, and 300 are AS numbers
- a community string; for example, "100:200", where 100 is the AS number and 200 is the community value

A regular expression is expressed as a combination of Terms and Operators. Regular expressions should always be enclosed in quotes.

The 7705 SAR also supports community expressions that allow the use of AND, OR, and NOT logical operators. For more information, see Community Expressions.

7.1.3.1 Terms

A term for an AS path regular expression is:

- an elementary term; for example, an AS number “200”
- a range term composed of two elementary terms separated by the “-” character, such as “200-300”
- the “.” dot wildcard character, which matches any elementary term
- a regular expression enclosed in parentheses “( )”
- a regular expression enclosed in square brackets used to specify a set of choices of elementary or range terms; for example, [100-300 400] matches any AS number between 100 and 300 or the AS number 400

A term for a community string regular expression is a string that is evaluated character by character and is composed of:

- an elementary term, which for a community string is any single digit, such as “4”
- a range term composed of two elementary terms separated by the “-” character, such as “2-3”
- a colon “:” to delimit the AS number from the community value
- the “.” dot wildcard character, which matches any elementary term or “:”
- a regular expression enclosed in parentheses “( )”
- a regular expression enclosed in square brackets, which is used to specify a set of choices of elementary or range terms; for example, [1-3 7] matches any single digit between 1 and 3 or the digit 7

7.1.3.2 Operators

The regular expression operators are listed in Table 120.

Table 120 **Regular Expression Operators**

Operator	Description
|	Matches the term on alternate sides of the pipe
.	Matches any elementary term or “:” community string
*	Matches multiple occurrences of the term
?	Matches 0 or 1 occurrence of the term
+	Matches 1 or more occurrence of the term

Table 120 **Regular Expression Operators (Continued)**

Operator	Description
( )	Used to parenthesize so a regular expression is considered as one term
[ ]	Used to demarcate a set of elementary or range terms
-	Used between the start and end of a range
{*m*,*n*}	Matches at least *m* and at most *n* repetitions of the term
{*m*}	Matches exactly *m* repetitions of the term
{*m*,}	Matches *m* or more repetitions of the term
:	Delimits the AS number from the community value — only allowed for communities
^	Matches the beginning of the string — only allowed for communities
$	Matches the end of the string — only allowed for communities
\	An escape character to indicate that the following character is a match criteria and not a grouping delimiter

Examples of AS path and community string regular expressions are listed in Table 121.

Table 121 **AS Path and Community Regular Expression Examples**

AS Path to Match Criteria	Regular Expression	Examples of Matches
Null AS path	**null** [1]	Null AS path
AS path is 11	**11**	11
AS path is 11 22 33	**11 22 33**	11 22 33
Zero or more occurrences of AS number 11	**11***	Null AS path 11 11 11 11 11 11 11 … 11
Path of any length that begins with AS numbers 11, 22, 33	**11 22 33 .***	11 22 33 11 22 33 400 500 600

Table 121 **AS Path and Community Regular Expression Examples (Continued)**

AS Path to Match Criteria	Regular Expression	Examples of Matches
Path of any length that ends with AS numbers 44, 55, 66	**.* 44 55 66**	44 55 66 100 44 55 66 100 200 44 55 66 100 200 300 44 55 66 100 200 300 … 44 55 66
One occurrence of the AS numbers 100 and 200, followed by one or more occurrences of the number 33	**100 200 33+**	100 200 33 100 200 33 33 100 200 33 33 33 100 200 33 33 33 … 33
One occurrence of the AS number 11, followed by one or more occurrences of AS number 22, followed by one or more occurrences of AS number 33	**11+ 22+ 33+**	11 22 33 11 11 22 33 11 11 22 22 33 11 11 22 22 33 33 11 ... 11 22 ... 22 33 ... 33
Path whose second AS number must be 11 or 22	**(. 11) | (. 22) .*** or **. (11 | 22) .***	100 11 200 22 300 400 …
Path of length one or two whose second AS number might be 11 or 22	**. (11 | 22)?**	100 200 11 300 22
Path whose first AS number is 100 and second AS number is either 11 or 22	**100 (11 | 22) .***	100 11 100 22 200 300
AS path 11, 22, or 33	**[11 22 33]**	11 22 33
Range of AS numbers to match a single AS number	**10-14**	Null AS path 10 or 11 or 12
	[10-12]*	Null AS path 10 or 11 or 12 10 10 or 10 11 or 10 12 11 10 or 11 11 or 11 12 12 10 or 12 11 or 12 12 …
Zero or one occurrence of AS number 11	**11? or 11{0,1}**	Null AS path 11

Table 121 **AS Path and Community Regular Expression Examples (Continued)**

AS Path to Match Criteria	Regular Expression	Examples of Matches
One through four occurrences of AS number 11	**11{1,4}**	11 11 11 11 11 11 11 11 11 11
One through four occurrences of AS number 11 followed by one occurrence of AS number 22	**11{1,4} 22**	11 22 11 11 22 11 11 11 22 11 11 11 11 22
Path of any length, except nonexistent, whose second AS number can be anything, including nonexistent	**. .* or . .{0,}**	100 100 200 11 22 33 44 55
AS number is 100 and community value is 200	**^100:200$**	100:200
AS number is 11 or 22 and community value is any number	**^((11)|(22)):(.*)$**	11:100 22:100 11:200 …
AS number is 11 and community value is any number that starts with 1	**^11:(1.*)$**	11:1 11:100 11:1100
AS number is any number and community value is any number that ends with 1, 2, or 3	**^(.*):(.*[1-3])$**	11:1 100:2002 333:55553 …
AS number is 11 or 22 and community value is any number that starts with 3 and ends with 4, 5 or 9	**^((11)|(22)):(3.*[459])$**	11:34 22:3335 11:3777779 …
AS number is 11 or 22 and community value ends in 33 or 44	**[^((11|22)):(.*((33)|(44)))$**	11:33 22:99944 22:555533 …

Note:

1. The null keyword matches an empty AS path.

7.1.4 Community Expressions

A community expression is a collection of community IDs separated by AND, OR, and NOT operations. A community expression is not the same as a regular expression. A community expression must be enclosed within quotes (“expression”) and may include parentheses to group expressions. An example of a community expression CLI command is:

config>router>policy-option>community "comm-name" expression "(2:2 AND 3:3) AND 4:4 AND NOT(1:1)"

For more information, see the community command description.

7.1.5 BGP and OSPF Route Policy Support

BGP and OSPF require route policy support. Figure 16, Figure 17, and Figure 18 show how route policies are evaluated in each protocol. Figure 16 shows BGP support, which applies a route policy as an internal part of the BGP route selection process. Figure 17 shows OSPF support for export policies, which applies routing policies at the edge of the protocol in order to control only the routes that are announced to or accepted from the Routing Table Manager (RTM). Figure 18 shows OSPF support for import policies, which applies import routing policies to control which routes are added to the OSPF route table after SPF is run.

Figure 16 **BGP Route Policy Diagram**

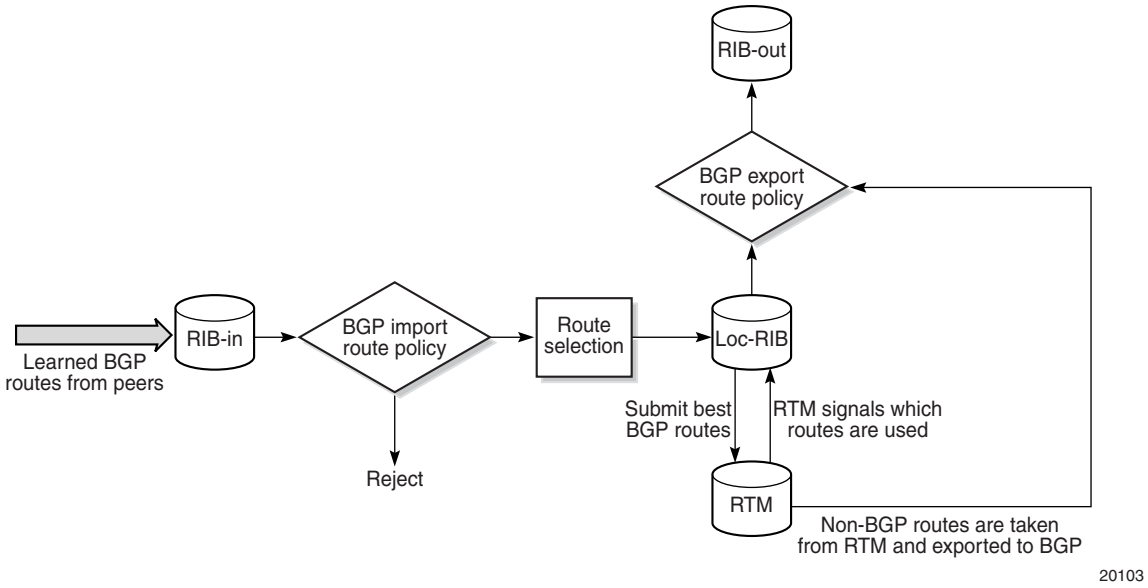


Figure 17 **OSPF Export Route Policy Diagram**

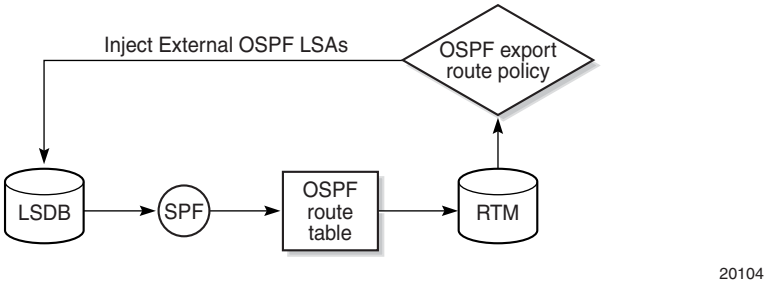
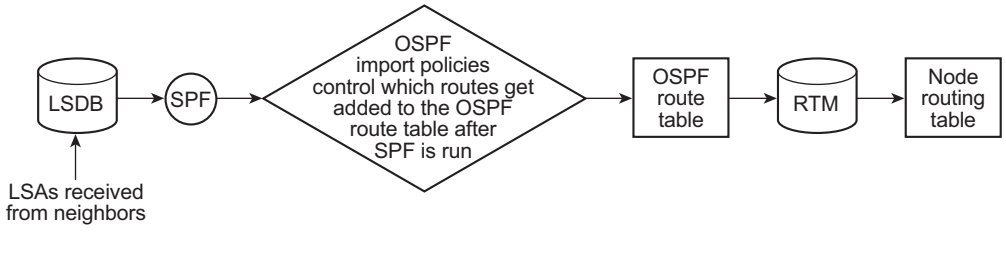


Figure 18 **OSPF Import Route Policy Diagram**



7.1.5.1 BGP Route Policies

The Nokia implementation of BGP uses route policies extensively. The implied or default route policies can be overridden by customized route policies. The default BGP properties, with no route policies configured, function as follows:

- accept all BGP routes into the RTM for consideration
- announce all used BGP learned routes to other BGP peers
- announce none of the IGP, static, or local routes to BGP peers

7.1.5.2 Readvertised Route Policies

Occasionally, within the network and as applicable to the VPRN service, BGP routes may be readvertised from BGP into OSPF and IS-IS. OSPF export policies (policies control which routes are exported to OSPF) are not handled by the main OSPF task but are handled by a separate task or an RTM task that filters the routes before they are presented to the main OSPF task.

7.1.5.3 Route Policies for BGP Next-Hop Resolution and Peer Tracking

The 7705 SAR can attach a route policy to the BGP next-hop resolution process and can allow a route policy to be associated with the optional BGP peer-tracking function. These two features are supported for BGP and VPRN BGP services.

7.1.5.3.1 BGP Next-Hop Resolution Policy Overview

BGP next-hop resolution is a fundamental part of BGP protocol operation. It determines the best matching route (or tunnel) for the BGP next-hop address and uses information about this resolving route when running the best-path selection algorithm and programming the forwarding table. Attaching a policy to BGP next-hop resolution provides additional control over which IP routes in the routing table can become resolving routes.

See Route Policy Support for BGP Next-Hop Resolution for details.

7.1.5.3.2 BGP Peer Tracking Policy Overview

Peer tracking is a BGP feature that triggers teardown of a BGP session if there is no IP reachability to the neighbor address or if the best matching IP route is rejected by the peer-tracking policy. This feature is configurable down to the peer level and is disabled by default. Peer tracking accelerates routing reconvergence when a failure leads to hold-timer expiry on the BGP session. BFD for BGP sessions has a similar function and is often used instead of peer tracking.

In the BGP implementation, an IPv4 or IPv6 neighbor address is considered reachable by the peer-tracking algorithm if there is any active and eligible IP route that matches the neighbor address. Policy support for peer tracking is useful so that the network administrator can restrict the set of eligible routes used to determine the reachability of an IPv4 or IPv6 BGP neighbor address when peer tracking is enabled.

See Route Policy Support for BGP Peer Tracking for details.

7.1.5.3.3 Route Policy Support for BGP Next-Hop Resolution

A route policy can be used for BGP next-hop resolution through the use of the **policy** command in the **config>router>bgp>next-hop-resolution** and **config>service>vprn>bgp>next-hop-resolution** contexts. The **policy** command specifies the route policy to be used.

If the BGP configuration references a next-hop resolution policy (for example, policy1) and BGP has an unlabeled unicast IPv4 or IPv6 route with IPv4 or IPv6 next-hop address *nh1* that is resolvable by an IP route from the RTM, BGP determines the resolving route for *nh1* as follows.

1. BGP looks for the most specific IP route in the candidate set that matches *nh1* (call this route R1). If there is no matching, route the BGP route is unresolved and the process is exited.
2. If R1 is rejected by an entry or the **default-action** of policy1, the route is unresolved and the process is exited.
3. If R1 is accepted by an entry or the **default-action** of policy1, R1 is the resolving route.

All policy actions are supported in a next-hop resolution policy; however, the following points should be noted:

- **next-policy** is ignored and matching routes are handled as per the default-action. Chaining multiple policies is not supported by this feature.
- **next-entry** is supported and causes evaluation of the policy to continue on to the next entry or the default-action is applied if this is the last entry

- no route attributes are modified as part of an **accept** action. The route is accepted but no modification of the AIGP metric, AS path, community, damping parameters, local preference, MED, next-hop, origin, and so on, occurs.

When **no default-action** is explicitly configured by the user, the implicit **default-action** is **accept**.

All **from** match conditions are supported in a next-hop resolution policy except as noted below:

- *family* is ignored. When resolving an IPv4 BGP route, only IPv4 routes are eligible for resolving the next hop and when resolving an IPv6 BGP route, only IPv6 routes are eligible for resolving the next hop. This logic cannot be changed by policy.
- *group-address*, *host-ip*, and *source-address* are ignored because they pertain only to multicast routes

The default next-hop resolution policy, used when the configuration has no policy, is equivalent to a user-configured policy with no entries and a default-action of **accept**.

It is possible to add, remove, or change the next-hop resolution policy at any time, without requiring BGP to first be shut down. The new policy is processed immediately and any indirect next-hop resolution changes that result from the new policy are immediately pushed down to the datapath.

7.1.5.3.4 Route Policy Support for BGP Peer Tracking

A route policy can be used for BGP peer tracking through the use of the **peer-tracking-policy** command in the **config>router>bgp** and **config>service>vprn>bgp** contexts. The **policy** command specifies the route policy to be used.

If the command references a policy (for example, policy1) and peer tracking is enabled with a BGP neighbor A having IPv4 or IPv6 address *p1*, the route BGP uses to determine the reachability of *p1* is determined as follows.

1. BGP initializes the set of candidate IP routes to all active routes installed in the forwarding table, excluding aggregate routes.
2. BGP looks for the most specific IP route in the candidate set that matches *p1* (call this route R1). If there is no matching route, the peer is unreachable and the process is exited.
3. If R1 is a BGP route or R1 is rejected by an entry or the default-action of policy1, the peer is unreachable and the process is exited.

4. If R1 is accepted by an entry or the default-action of policy1, the peer is reachable via R1.

If the above algorithm determines that the peer is unreachable, the BGP session with A is closed after a 1-second delay to dampen route flaps and stays closed until there is a route R1 that is accepted (that is, meets the step 4 condition). Reachability is evaluated before a new session is established, whenever the most specific route that matches the neighbor address changes, and whenever there is a change to the peer-tracking policy.

All policy actions are supported in a peer-tracking policy; however, the following points should be noted:

- **next-policy** is ignored and matching routes are handled per the default-action. Chaining multiple policies is not supported by this feature.
- **next-entry** is supported and causes evaluation of the policy to continue on to the next entry or the default-action is applied if this is the last entry
- no route attributes are modified as part of an **accept** action. The route is accepted but no modification of the AIGP metric, AS path, community, damping parameters, local preference, MED, next-hop, origin, and so on, occurs.

When **no default-action** is explicitly configured by the user, the implicit **default-action** is **accept**.

All **from** match conditions are supported in a peer-tracking policy except as noted below:

- *family* is ignored. When determining the reachability of an IPv4 peer address, only IPv4 routes are eligible and when determining the reachability of an IPv6 peer address, only IPv6 routes are eligible. This logic cannot be changed by policy.
- *group-address*, *host-ip*, and *source-address* are ignored because they pertain only to multicast routes

The default peer-tracking policy, used when the configuration has no peer-tracking policy, is equivalent to a user-configured policy with no entries and a default-action of **accept**.

It is possible to add, remove, or change the peer-tracking policy at any time, without requiring BGP to first be shut down. The new policy is processed immediately and this may trigger one or more sessions to be torn down.

7.1.6 When to Use Route Policies

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

- to control the protocol to allow all routes to be imported into the routing table. This enables the routing table to learn about particular routes to enable packet forwarding and redistributing of routes into other routing protocols.
- to control the export of a protocol's learned active routes
- to enable the MP-BGP routing protocol to announce active routes learned from another routing protocol (that is, the static routes configured in the 7705 SAR). This function is sometimes called route redistribution.
- to allow unique behaviors to control route characteristics; for example, change the route preference, AS path, or community values to manipulate or control the route selection
- to control BGP route flapping by use of route flap damping

7.1.7 Troubleshooting the FIB

Adapter cards that are installed in a 7705 SAR-8 Shelf V2 or 7705 SAR-18 chassis may have different hardware limitations with respect to IPv4 and IPv6 FIB routing. Alarms may be generated on the node when IPv4 or IPv6 routing faults related to scaling, capability, or a datapath route lookup problem are detected on an adapter card. Table 122 lists the applicable alarms.

Table 122 **FIB Alarms**

Alarm	Description
"Class MDA Module : runtime event, details: Fatal FIB_STATUS_IPV6_UNSUPPORTED_SUBNET_MASK Error Detected!"	A /65 to /127 IPv6 route was downloaded to an adapter card without hardware support
"Class MDA Module : runtime event, details: Fatal FIB_STATUS_IPV4_SCALE_EXCEEDED Error Detected!"	The total number of IPv4 routes in the FIB exceeds the adapter card hardware capability
"Class MDA Module : runtime event, details: Fatal FIB_STATUS_IPV4_VRF_SCALE_EXCEEDED Error Detected!"	The total number of IPv4 routing instances in the FIB (for example, number of VPRNs) exceeds the adapter card hardware capability
"Class MDA Module : runtime event, details: Fatal FIB_STATUS_IPV6_SCALE_EXCEEDED Error Detected!"	The total number of IPv6 routes in the FIB exceeds the adapter card hardware capability

Table 122 **FIB Alarms (Continued)**

Alarm	Description
“Class MDA Module : runtime event, details: Fatal FIB_STATUS_IPV6_VRF_SCALE_EXCEEDED Error Detected!”	The total number of IPv6 routing instances in the FIB (for example, number of VPRNs) exceeds the adapter card hardware capability
“Class MDA Module : runtime event, details: Fatal FIB_STATUS_IPV4_DP_LOOKUP_FAULT Error Detected!”	The software has detected faults with datapath IPv4 route lookups

If any of the alarms in Table 122 are generated, the IPv4 or IPv6 datapath on the adapter card will operate in a random way. For example, traffic may continue to flow as expected in some cases, but in other cases, traffic could be blackholed or misrouted.

The **show router fib 1 ipv4 summary** and **show router fib 1 ipv6 summary** commands can be used to confirm that the FIB limits are exceeded.

For example:

```
# show router fib 1 ipv4 summary

===============================================================================
FIB Summary
===============================================================================
                              Active
-------------------------------------------------------------------------------
Static                        0
Direct                        142
HOST                          0
BGP                           0
BGP VPN                       38569
OSPF                          234
ISIS                          486
RIP                           0
Aggregate                     0
Sub Mgmt                      0
-------------------------------------------------------------------------------
Total Installed               39431
-------------------------------------------------------------------------------
Current Occupancy             120%
Overflow Count                0
Suppressed by Selective FIB   0
Occupancy Threshold Alerts
    Alert Raised 1 Times; Last Alert 11/30/2016 07:50:46
===============================================================================
```

To restore a FIB that is in a failed state, the user must do the following.

Step 1. If possible, resolve the condition that led to the alarm being generated. For example, for scaling alarms, reduce the size of the routing table below the maximum for the affected adapter card.

Step 2. Execute the **tools perform mda-table-refresh** command to restore the FIB. Refer to the 7705 SAR OAM and Diagnostics Guide, “Tools Perform Commands” for a command description.

Wait a few minutes to ensure that no new alarm is raised; if there are no new alarms, the fault has been successfully resolved.

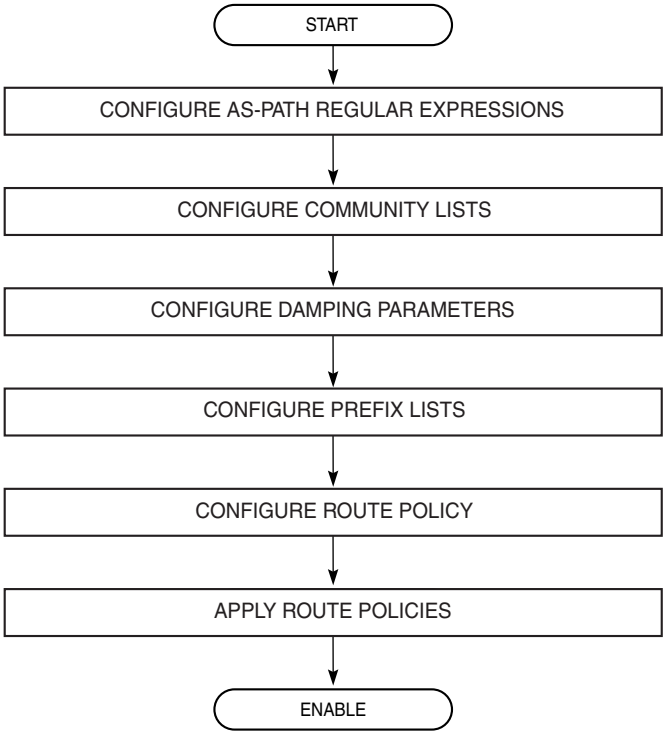
If a new alarm is raised, this indicates that the adapter card must be replaced.

Alternatively, when an alarm is generated, replace the card with a new adapter card that supports the higher scaling limit (for scaling alarms) or replace the card to resolve persistent datapath lookup faults.

7.2 Route Policy Configuration Process Overview

Figure 19 displays the process to provision basic route policy parameters.

Figure 19 **Route Policy Configuration and Implementation Flow**



7.3 Configuration Notes

When configuring policy statements, the policy statement name must be unique.

7.3.1 Reference Sources

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

7.4 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
- Basic Route Policy Configuration
- Configuring Route Policy Components
- Route Policy Configuration Management Tasks

7.5 Route Policy Configuration Overview

Route policies allow you to configure routing according to specifically defined policies. You can create policies and entries to allow or deny paths based on parameters such as source address, destination address, protocol, and community list.

Policies can be as simple or complex as required. A simple policy can block routes for a specific location or IP address. More complex policies can be configured using numerous policy statement entries containing matching conditions to specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

7.5.1 When to Create Routing Policies

Route policies are created in the **config>router** context. There are no default route policies. Each route policy must be explicitly created and applied. Applying route policies can introduce more efficiency as well as more complexity to the capabilities of the 7705 SAR.

Route policies are used to control which MPLS labels should be learned or advertised. Based on the configured routing policy, MPLS labels from certain neighbors can be discarded.

Route policies are also used to control the size and content of the BGP, OSPF, and IS-IS routing tables, the routes that are advertised, and the best route to take to reach a destination.

Route policies can be created to control:

- a protocol to export all the active routes learned by that protocol
- route characteristics to control which route is selected to act as the active route to reach a destination and advertise the route to neighbors
- the protocol to import all routes into the routing table. A routing table must learn about particular routes to be able to forward packets and redistribute to other routing protocols.
- damping

Before a route policy is applied, analyze the policy's purpose and be aware of the results (and consequences) when packets match the specified criteria and the associated actions and default actions, if specified, are executed. Membership reports can be filtered based on a specific source address.

7.5.2 Default Route Policy Actions

Routing protocols have default behaviors for the import and export of routing information.

For BGP, OSPF, and IS-IS, the default route policy actions are as follows:

- BGP
  - import – all routes from BGP peers are accepted and passed to the BGP route selection process
  - export (internal routes) – all active BGP routes are advertised to BGP peers
  - export (external routes) – all non-BGP learned routes are not advertised to BGP peers
- OSPF
  - import – all OSPF routes are accepted from OSPF neighbors
  - export (internal routes) – all OSPF routes are automatically advertised to all neighbors
  - export (external routes) – all non-OSPF learned routes are not advertised to OSPF neighbors
- IS-IS
  - import – not applicable; all IS-IS routes are accepted from IS-IS neighbors and cannot be controlled by route policies
  - export (internal routes) – all IS-IS routes are automatically advertised to all neighbors
  - export (external routes) – all non-IS-IS learned routes are not advertised to IS-IS neighbors

7.5.3 Policy Evaluation

Routing policy statements can consist of one or several entries. The entries specify the matching criteria. A label is compared to the first entry in the policy statement. If it matches, the specified entry action is taken, either accepted or rejected. If the action is to accept or reject the label, that action is taken and the evaluation of the label ends.

If the label does not match the first entry, the label is compared to the next entry (if more than one is configured) in the policy statement. If there is a match with the second entry, the specified action is taken. If the action is to accept or reject the label, that action is taken and the evaluation of the label ends, and so on.

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

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

Route policies can also match a given route policy entry and continue to search for other entries within either the same route policy or the next route policy by specifying the next-entry or next-policy option in the entry's **action** command. Policies can be constructed to support multiple states to the evaluation and setting of various route attributes.

Figure 20 shows an example of the route policy process.

Figure 21 shows the next-entry and next-policy route policy processes. The next-entry logic is that for each policy statement, the process checks each entry until the first match is hit, at which point the appropriate action is taken, which could be next-policy.

Figure 20 **Route Policy Process Example**

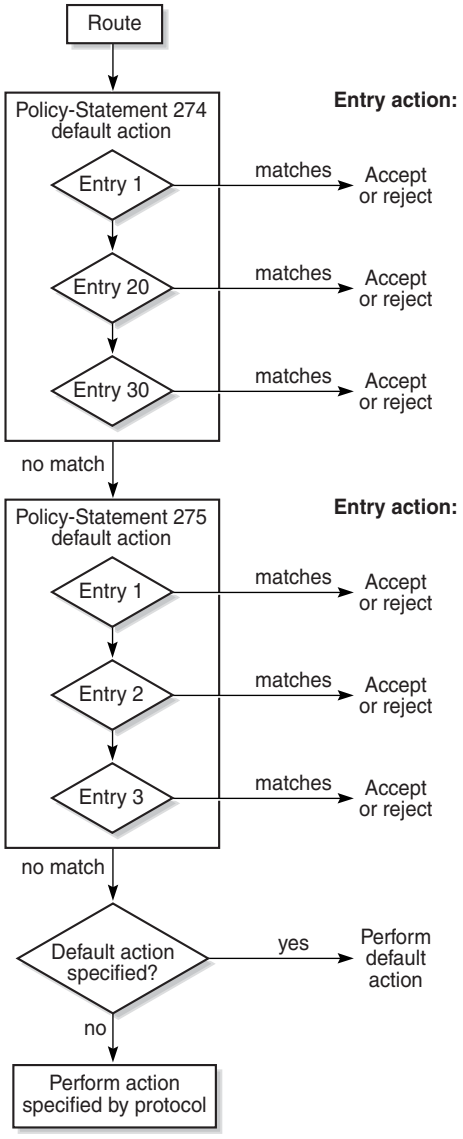
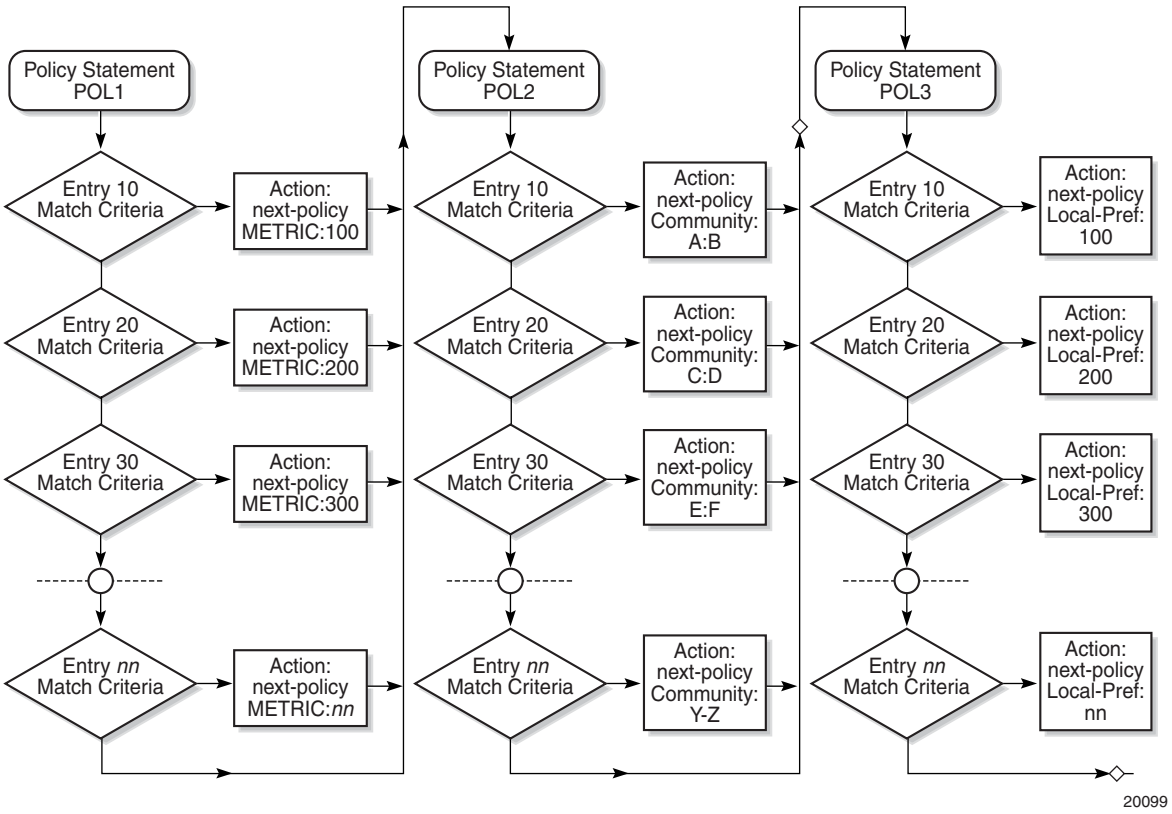


Figure 21 **Next Entry and Next Policy Logic Example**



7.5.3.1 Damping

Damping initiates controls when routes flap. Route flapping can occur when an advertised route between nodes alternates (flaps) back and forth between two paths due to network problems that cause intermittent route failures. To limit processing requirements, the amount of routing state change updates propagated must be reduced. Thus, when a route flaps beyond a configured value (the suppress value), then that route is removed from the routing table and routing protocols until the value falls below the reuse value.

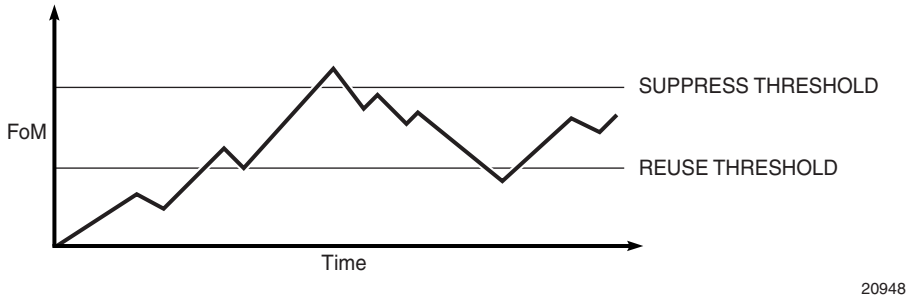
A route can be suppressed according to the Figure of Merit (FoM) value. The FoM is a value that is added to a route each time it flaps. A new route begins with an FoM value of 0.

Damping is optional. If damping is configured, the following parameter values must be explicitly specified because there are no default values:

- suppress
- half-life
- reuse
- max-suppress

When a route's FoM value exceeds the suppress value, the route is removed from the routing table. The route is considered to be stable when the FoM drops below the reuse value by means of the specified half-life parameter. The route is then returned to the routing tables. When routes have higher FoM and half-life values, they are suppressed for longer periods of time. Figure 22 depicts an example of a flapping route, the suppress threshold, the half-life decay (time), and reuse threshold. The peaks represent route flaps, and the slopes represent half-life decay.

Figure 22 **Damping Example**



7.6 Basic Route Policy Configuration

This section provides information on configuring route policies and shows configuration examples of common tasks.

The minimum route policy parameters that need to be configured are:

- policy statement with the following parameters specified:
  - at least one entry
  - entry action

The following is an example of route policy configuration, including examples for defining community members, community expressions, and the as-path regular expressions.

```
A:ALU-B>config>router>policy-options# info
----------------------------------------------
       community "all-types" members "5000:[1-6][1-9][0-9]"
       community "all-normal" members "5000:[1-5][1-9][0-9]"
       community "comm-expression-1" expression "target:1234:111 OR target:1234:222"
       community "comm-expression-2" expression "target:555:100 AND target:555:600"
. . .
       as-path "Outside madeup paths" expression ".* 5001 .*"
       as-path "Outside Internet paths" expression ".* 5002 .*"
       policy-statement "RejectOutsideASPaths"
           entry 1
               from
                   protocol bgp
                   as-path "Outside madeup paths"
               exit
               action reject
               exit
           exit
           entry 2
               from
                   protocol bgp
                   as-path "Outside Internet paths"
               exit
               action reject
               exit
           exit
           entry 3
               from
                   protocol ospf
               exit
               to
                   protocol bgp
               exit
               action reject
               exit
           exit
```

```
            entry 4
                from
                    protocol isis
                exit
                to
                    protocol bgp
                exit
                action reject
                exit
            exit
            default-action accept
            exit
        exit
        policy-statement "aggregate-customer-peer-only"
            entry 1
                from
                    community "all-customer-announce"
                exit
                action accept
                exit
            exit
            default-action reject
            exit
            exit
-------------------------------------------
A:ALU-B>config>router>policy-options#
```

7.7 Configuring Route Policy Components

Use the CLI syntax displayed below to configure the following:

- Beginning the Policy Statement
- Creating a Route Policy
- Configuring a Default Action
- Configuring an Entry
- Configuring an AS Path (policy-option)
- Configuring a Community List or Expression
- Configuring Damping
- Configuring a Prefix List
- Configuring PIM Join/Register Policies
- Configuring Bootstrap Message Import and Export Policies
- Configuring LDP-to-Segment Routing Stitching Policies

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]
```

7.7.1 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.

7.7.2 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 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#
```

7.7.3 Configuring a Default Action

Specifying a default action is optional. The default action controls those packets not matching any policy statement entries. The default action is applied only to those routes that do not match any policy entries.

If no default action is specified and there is no match, the packets will be accepted.

A policy statement must include at least one entry (see Configuring an Entry).

To enter the mode to create or edit route policies, you must enter the **begin** keyword at the **config>router>policy-options** prompt. Other editing commands include:

- the **commit** command, which saves changes made to route policies during a session
- the **abort** command, which discards changes made to route policies during a session

CLI Syntax:

```
config>router>policy-options
   begin
   commit
   abort
   policy-statement name
      default-action {accept |next-entry |
        next-policy | reject}
        aigp-metric metric
        aigp-metric metric add
        aigp-metric igp
        as-path {add | replace} name
        as-path-prepend as-path [repeat]
        community {add | remove | replace} name
           [name...(up to 28 max)]
        damping {name | none}
        local-preference local-preference
        metric {add | subtract} metric
        metric set {igp | metric}
        next-hop ip-address
        next-hop-self
        origin {igp | egp |incomplete}
        preference preference
        tag tag
        type type
```

The following example displays default action configuration command usage. These commands are configured in the **config>router>policy-options** context.

Example:

```
config>router>policy-options# policy-statement "1"
policy-statement$ default-action accept
```

The following example displays the default action configuration:

```
A:ALU-B>config>router>policy-options# info
----------------------------------------------
           policy-statement "1"
               default-action accept
                   as-path add "saratoga"
                   community add "365"
                   damping "flaptest"
                   metric igp
```

```
                        next-hop 10.10.10.104
                    exit
                        type 1
                exit
-------------------------------------------
A:ALU-B>config>router>policy-options#
```

7.7.4 Configuring an Entry

An entry action must be specified. The other parameters in the **entry>action** context are optional.

The **from>community** and **from>community expression** commands are mutually exclusive for a specific entry. The last **community** command entered overwrites any previous **community** command.

CLI Syntax:

```
config>router>policy-options
   begin
   commit
   abort
   policy-statement name
      entry entry-id
         description text
         action {accept | next-entry | next-policy |
            reject}
            aigp-metric metric
            aigp-metric metric add
            aigp-metric igp
            as-path {add | replace} name
            as-path-prepend as-path [repeat]
            community {add | remove | replace} name
               [name...(up to 28 max)]
            damping {name | none}
            local-preference local-preference
            metric {add | subtract} metric
            metric set {igp | metric}
            next-hop ip-address
            next-hop-self
            origin {igp | egp |incomplete}
            preference preference
            tag tag
            type type
         description description-string
         from
            area area-id
            as-path {add | replace} name
            community comm-name
```

```
            community expression expression
            external
            family [ipv4] [vpn-ipv4]
            group-address prefix-list-name
            interface interface-name
            level {1 | 2}
            neighbor {ip-address | prefix-list name}
            origin {igp | egp | incomplete | any}
            prefix-list name [name...(up to 5 max)]
            protocol protocol [all | instance instance]
            source-address ip-address
            tag tag
            type type
          to
            level {1 | 2}
            neighbor {ip-address | prefix-list name}
            prefix-list name [name...(up to 5 max)]
            protocol protocol [all | instance instance]
```

The following example displays entry command usage. These commands are configured in the **config>router>policy-options** context.

Example:

```
config>router>policy-options# policy-statement "1"
policy-statement# entry 1
policy-statement>entry$ to
policy-statement>entry>to# protocol bgp
policy-statement>entry>to# neighbor 10.10.10.104
policy-statement>entry>to# exit
policy-statement>entry# action accept
policy-statement>entry>action# exit
policy-statement>entry# exit
policy-statement# entry 2
policy-statement>entry$ from
policy-statement>entry>from# protocol ospf
policy-statement>entry>from# exit
policy-statement>entry$ to
policy-statement>entry>to# protocol ospf
policy-statement>entry>to# neighbor 10.10.0.91
policy-statement>entry>to# exit
policy-statement>entry# action accept
policy-statement>entry>action# exit
```

The following example displays entry parameters and includes the default action parameters that were displayed in the previous section.

```
A:ALU-B>config>router>policy-options# info
----------------------------------------------
            policy-statement "1"
                entry 1
```

```
                    to
                         protocol bgp
                         neighbor 10.10.10.104
                    exit
                    action accept
                    exit
                exit
                entry 2
                    from
                        protocol ospf
                    exit
                    to
                        protocol ospf
                        neighbor 10.10.0.91
                    exit
                    action accept
                    exit
                exit
                default-action accept
                    . . .
                exit
            exit
-------------------------------------------
```

7.7.5 Configuring an AS Path (policy-option)

An AS path is defined by a regular expression in the **config>router>policy-options** context. Once defined, it can be added, removed, or replaced in a policy statement as part of a default action, an entry action, or an entry from (source) definition. See Configuring a Default Action and Configuring an Entry.

The following example displays **as-path** command usage.

```
A:ALU-B>config>router># info
-----------------------------------------------
    . . .
       as-path "Outside madeup paths" expression ".* 5001 .*"
       as-path "Outside Internet paths" expression ".* 5002 .*"
    . . .
-----------------------------------------------
A:ALU-B>config>router>#
```

7.7.6 Configuring a Community List or Expression

Community lists are composed of a group of destinations that share a common property. Community lists allow you to administer actions on a configured group instead of having to execute identical commands for each member.

Community expressions are logical expressions composed of community lists (community IDs) separated by AND, OR, and NOT operations. Community expressions provide flexible matching of communities.

Community lists and expressions must be enclosed within quotes.

The following example displays community list and community expression configurations:

```
A:ALU-B>config>router>policy-options# info
----------------------------------------------
     community "eastern" members "100:200"
     community "western" members "100:300"
     community "northern" members "100:400"
     community "southern" members "100:500"
     community "headquarters" members "100:1000"
     community "manor" expression "target:100:111"
     community "manor2" expression "target:100:111 AND target:100:555"
     policy-statement "1"
          entry 1
               to
                    protocol bgp
                    neighbor 10.10.10.104
               exit
          entry 10
               from
                    community expression "NOT ([eastern] OR [western])"
               exit
               action accept
....
----------------------------------------------
```

7.7.7 Configuring Damping

Observe the following when configuring damping.

- For each damping profile, all parameters must be configured.
- The suppress value must be greater than the reuse value (see Figure 22).
- Damping is enabled in the **config>router>bgp** context at the BGP global, group, and neighbor levels. If damping is enabled but route policy does not specify a damping profile, the default damping profile is used. This default profile is always present and consists of the following parameters:
  - half-life: 15 min
  - max-suppress: 60 min
  - reuse: 750
  - suppress: 3000

Use the following CLI syntax to configure damping:

CLI Syntax:
```
config>router>policy-options
   damping name
      half-life minutes
      max-suppress minutes
      reuse integer
      suppress integer
```

The following example displays damping configuration command usage.

Example:
```
config>router>policy-options#
config>router>policy-options#damping damptest123
config>router>policy-options#damping# max-suppress 60
config>router>policy-options#damping# half-life 15
config>router>policy-options#damping# re-use 750
config>router>policy-options#damping# suppress 1000
config>router>policy-options#damping# exit
config>router>policy-options#
```

The following example displays a damping configuration:

```
A:ALU-B>config>router>policy-options# info
----------------------------------------------
     damping "damptest123"
          half-life 15
          max-suppress 60
          reuse 750
          suppress 1000
     exit
----------------------------------------------
A:ALU-B>config>router>policy-options#
```

7.7.8 Configuring a Prefix List

Use the following CLI syntax to configure a prefix list:

CLI Syntax:
```
prefix-list name
   prefix ip-prefix/prefix-length [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 10.10.0.1/8
policy-options>prefix-list# prefix 10.10.0.2/8
policy-options>prefix-list# prefix 10.10.0.3/8
policy-options>prefix-list# prefix 10.10.0.4/8
```

The following example displays the prefix list configuration.

```
A:ALU-B>config>router>policy-options# info
----------------------------------------------
            prefix-list "western"
                    prefix 10.10.0.1/8 exact
                    prefix 10.10.0.2/8 exact
                    prefix 10.10.0.3/8 exact
                    prefix 10.10.0.4/8 exact
            exit
----------------------------------------------
A:ALU-B>config>router>policy-options>#
```

7.7.9 Configuring PIM Join/Register Policies

Join policies are used in Protocol Independent Multicast (PIM) configurations to prevent the transport of multicast traffic across a network and the dropping of packets at a router at the edge of the network. PIM Join filters reduce the potential for denial of service (DoS) attacks and PIM state explosion—large numbers of Join messages forwarded to each router on the RPT, resulting in memory consumption.

Register policies are used to prevent any unwanted sources from transmitting multicast streams. You can apply register policies at the RP, or at the edge so that register data does not travel unnecessarily over the network towards the RP.

For information on importing a Join/Register policy into a PIM configuration, see the “PIM-SM Routing Policies” and “Importing PIM Join/Register Policies” sections in the 7705 SAR Routing Protocols Guide.

Configuring a PIM join or register policy follows the same process as that for any other policy. However, when configuring an entry, include the **entry>from>group-address** and **entry>from>source-address** commands. See Configuring an Entry for the CLI syntax.

The (*,G) or (S,G) information is used to forward unicast or multicast packets.

- **group-address** matches the group in join/prune messages

  ```
  group-address 239.255.50.208/16 exact
  ```

- **source-address** matches the source in join/prune messages

  ```
  source-address 239.255.150.208/16 longer
  ```

- **interface** matches any join message received on the specified interface

  ```
  interface port 1/1/1
  ```

- **neighbor** matches any join message received from the specified neighbor

  ```
  neighbor 10.10.10.10
  ```

The following example displays the command usage for a PIM join policy named “pim_join”. The policy will not allow Join messages for group 239.50.50.208/32 and source 239.255.150.208/16, but will allow other Join messages. These commands are configured in the **config>router** context.

Example:

```
policy-options# begin
policy-options# policy-statement pim_join
policy-options>policy-statement$ entry 10
policy-options>policy-statement>entry$ from
policy-options>policy-statement>entry>from$ group-
 address 239.255.50.208/16
policy-options>policy-statement>entry>from$ source-
 address 239.255.150.208/16
policy-options>policy-statement>entry>from$ exit
policy-options>policy-statement>entry# action reject
policy-options>policy-statement>entry#
```

The following example displays a PIM register policy that allows registration for (*,239,255.0.0/8). These commands are configured in the **config>router** context.

Example:

```
policy-options# policy-statement reg_pol
policy-options>policy-statement$ entry 10
policy-options>policy-statement>entry$ from
policy-options>policy-statement>entry>from$ group-
 address 239.255.0.0/8
policy-options>policy-statement>entry# action accept
policy-options>policy-statement>entry>action# exit
policy-options>policy-statement>entry# exit
policy-options>policy-statement# exit
```

The following example displays the PIM join and register policy configurations:

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
...
     policy-statement "pim_join"
          entry 10
               from
                    group-address "239.50.50.208/32"
                    source-address 239.255.150.208
               exit
               action reject
          exit
     exit
```

```
        policy-statement "reg_pol"
             entry 10
                  from
                       group-address "239.255.0.0/8"
                  exit
                  action accept
             exit
        exit
...
-----------------------------------------------
```

7.7.10 Configuring Bootstrap Message Import and Export Policies

Bootstrap import and export policies are used to control the flow of bootstrap messages to and from the rendezvous point (RP).

The following configuration example specifies that there should be no BSR messages received or sent out of interface port 1/1/1. These commands are configured in the **config>router** context.

Example:
```
policy-options# policy-statement pim_import_policy
policy-options>policy-statement$ entry 10
policy-options>policy-statement>entry$ from
policy-options>policy-statement>entry>from$ interface
 port 1/1/1
policy-options>policy-statement>entry>from$ exit
policy-options>policy-statement>entry# action reject
policy-options>policy-statement>entry# exit
policy-options>policy-statement# exit
```

Example:
```
policy-options# policy-statement pim_export_policy
policy-options>policy-statement$ entry 10
policy-options>policy-statement>entry$ to
policy-options>policy-statement>entry>to$ interface port
 1/1/1
policy-options>policy-statement>entry# action reject
policy-options>policy-statement>entry# exit
policy-options>policy-statement# exit
```

The following configuration example illustrates the application of the policies to PIM. Up to five import and five export policies can be specified.

Example:
```
config>router>pim>rp# bootstrap-import pim_import_policy
config>router>pim>rp# bootstrap-export pim_export_policy
```

7.7.11 Configuring LDP-to-Segment Routing Stitching Policies

Use the following CLI syntax to configure route policy options to support LDP-to-Segment Routing (SR) stitching.

CLI Syntax:

```
config>router>policy-options
  begin
  prefix-list name
    prefix ip-prefix/prefix-length [exact | longer |
      through length | prefix-length-range length1-
      length2]
  policy-statement name
    entry entry-id
      from
        protocol isis
        prefix-list name
      to
        protocol ldp
      action {accept | next-entry | next-policy |
        reject}
```

The following is an example of LDP-to-SR stitching route policy options configuration.

Example:

```
config>router>policy-options# begin
config>router>policy-options# prefix-list "prefixes"
config>router>policy-options>prefix-list$ prefix
 198.51.100.0/24 longer
config>router>policy-options>prefix-list# exit
config>router>policy-options# policy-statement
 "export-SR"
config>router>policy-options>policy-statement# entry 10
config>router>policy-options>policy-statement>entry#
 from protocol isis
config>router>policy-options>policy-statement>entry#
 from prefix-list "prefixes"
config>router>policy-options>policy-
 statement>entry>from# exit
config>router>policy-options>policy-statement>entry# to
 protocol ldp
config>router>policy-options>policy-statement>entry>
 to# exit
config>router>policy-options>policy-statement>entry#
 action accept
config>router>policy-options>policy-
 statement>entry>action# exit
```

```
config>router>policy-options>policy-statement>entry#
 exit
config>router>policy-options# commit
config>router>policy-options# exit
```

The following example displays the LDP-to-SR stitching route policy options configuration.

```
A:NOK-1 Dut-B>config>router>policy-options# info
----------------------------------------------
        ...
            prefix-list "prefixes"
                prefix 198.51.100.0/24 longer
            exit
            policy-statement "export-SR"
                entry 10
                    from
                        protocol isis
                        prefix-list "prefixes"
                    exit
                    to
                        protocol ldp
                    exit
                    action accept
                    exit
                exit
            exit
----------------------------------------------
A:NOK-1 Dut-B>config>router>policy-options#
```

7.8 Route Policy Configuration Management Tasks

This section describes the following route policy configuration management tasks:

- Editing Policy Statements and Parameters
- Deleting an Entry
- Deleting a Policy Statement

7.8.1 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#
```

7.8.2 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
```

7.8.3 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
```

7.9 Route Policy Command Reference

7.9.1 Command Hierarchies

- Route Policy Configuration Commands
- Show Commands

7.9.1.1 Route Policy Configuration Commands

```
config
    — [no] router
        — [no] policy-options
            — abort
            — as-path name expression regular-expression
            — no as-path name
            — begin
            — commit
            — community name members comm-id [comm-id … (up to 15 max)]
            — community name expression expression [exact]
            — no community name [members comm-id]
            — [no] damping name
                — half-life minutes
                — no half-life
                — max-suppress minutes
                — no max-suppress
                — reuse integer
                — no reuse
                — suppress integer
                — no suppress
            — [no] policy-statement name
                — default-action {accept | next-entry | next-policy | reject}
                — no default-action
                    — aigp-metric metric
                    — aigp-metric metric add
                    — aigp-metric igp
                    — no aigp-metric
                    — as-path {add | replace} name
                    — no as-path
                    — as-path-prepend as-number [repeat]
                    — no as-path-prepend
                    — community add name [name...(up to 28 max)]
                    — community remove name [name...(up to 28 max)]
                    — community replace name [name...(up to 28 max)]
                    — no community
                    — damping {name | none}
                    — no damping
                    — local-preference local-preference
                    — no local-preference
                    — metric {add | subtract} metric
                    — metric set {igp | metric}
                    — no metric
                    — next-hop ip-address
                    — no next-hop
                    — [no] next-hop-self
                    — origin {igp | egp | incomplete}
                    — no origin
                    — preference preference
                    — no preference
                    — tag tag
                    — no tag
```

- **type** *type*
- **no type**

- **description** *description-string*
- **no description**
- **entry** *entry-id*
- **no entry**
  - **action** {**accept** | **next-entry** | **next-policy** | **reject**}
  - **no action**
    - **aigp-metric** *metric*
    - **aigp-metric** *metric* **add**
    - **aigp-metric igp**
    - **no aigp-metric**
    - **as-path** {**add** | **replace**} *name*
    - **no as-path**
    - **as-path-prepend** *as-number* [*repeat*]
    - **no as-path-prepend**
    - **community** {**add** *name* | **remove** *name* | **replace** *name*} [*name*...(up to 28 max)]
    - **no community**
    - **damping** {*name* | **none**}
    - **no damping**
    - **local-preference** *local-preference*
    - **no local-preference**
    - **metric** {**add** | **subtract**} *metric*
    - **metric set** {**igp** | *metric*}
    - **no metric**
    - **next-hop** *ip-address*
    - **no next-hop**
    - [**no**] **next-hop-self**
    - **origin** {**igp** | **egp** | **incomplete**}
    - **no origin**
    - **preference** *preference*
    - **no preference**
    - **tag** *tag*
    - **no tag**
    - **type** *type*
    - **no type**
  - **description** *description-string*
  - **no description**
  - [**no**] **from**
    - **area** *area-id*
    - **no area**
    - **as-path** *name*
    - **no as-path**
    - **community** *comm-name*
    - **community expression** *expression*
    - **no community**
    - [**no**] **external**
    - **family** [**ipv4**] [**vpn-ipv4**] [**label-ipv4**] [**bgp-ls**]
    - **no family**
    - **group-address** *prefix-list-name*
    - **no group-address**
    - **interface** *interface-name*
    - **no interface**

— **level** {**1** | **2**}
— **no level**
— **neighbor** {*ip-address* | **prefix-list** *name*}
— **no neighbor**
— **origin** {**igp** | **egp** | **incomplete** | **any**}
— **no origin**
— **prefix-list** *name* [*name*...(**up to 5 max**)]
— **no prefix-list**
— **protocol** *protocol* [**all** | {**instance** *instance*}]
— **protocol bgp bgp-label**
— **no protocol**
— **source-address** *ip-address*
— **no source-address**
— **tag** *tag*
— **no tag**
— **type** *type*
— **no type**
— [**no**] **to**
— **level** {**1** | **2**}
— **no level**
— **neighbor** {*ip-address* | **prefix-list** *name*}
— **no neighbor**
— **prefix-list** *name* [*name*...(up to 5 max)]
— **no prefix-list**
— **protocol** *protocol* [**all** | {**instance** *instance*}]
— **protocol bgp bgp-label**
— **no protocol**
— [**no**] **prefix-list** *name*
— [**no**] **prefix** *ip-prefix/prefix-length* [**exact** | **longer** | **through** *length* | **prefix-length-range** *length1-length2*]
— [**no**] **triggered-policy**

7.9.1.2 Show Commands

show
— **router** *router-name*
— **policy** [*name* | **damping** *name* | **prefix-list** *name* | **as-path** *name* | **community** *name* | **admin**]

7.9.2 Command Descriptions

7.9.2.1 Configuration Commands

- Generic Commands
- Route Policy Options
- Route Policy Damping Commands
- Route Policy Prefix Commands
- Route Policy Entry Match Commands
- Route Policy Action Commands

7.9.2.1.1 Generic Commands

abort

Syntax **abort**

Context config>router>policy-options

Description This command discards changes made to a route policy.

Default n/a

begin

Syntax **begin**

Context config>router>policy-options

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

Default n/a

commit

Syntax **commit**

Context config>router>policy-options

Description This command saves changes made to a route policy.

Default n/a

description

Syntax **description** *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 contents of the entity.

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

Default n/a

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.

7.9.2.1.2 Route Policy Options

as-path

Syntax **as-path** *name* **expression** *regular-expression*
no as-path *name*

Context config>router>policy-options

Description This command creates a route policy AS path regular expression statement to use in route policy entries. See Regular Expressions for information.

The **no** form of the command deletes the AS path regular expression statement.

Default no as-path

Parameters *name* — the AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

regular-expression — the AS path regular expression (any string or **null**)

Values any string up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

null — the AS path expressed as an empty regular expression string

community

Syntax **community** *name* **members** *comm-id* [*comm-id***...**(up to 15 max)]
community *name* **expression** *expression* [**exact**]
no community *name* [**members** *comm-id*]

Context config>router>policy-options

Description This command creates a route policy community list to use in route policy entries.

The **community** *name* **expression** form of the command extends the **community** *name* **members** form by allowing the community list structure to support AND, OR, and NOT operators.

When the **community** *name* **members** command is used, community lists operate with implicit AND support only, and all communities must match to provide a positive match, as shown in the following example, where the only routes that match include all three communities:

- **community** “north” **members** “target:1234:111” “target:1234:222” “target:1234:333”

Using the **community** *name* **expression** command allows for configuration of a community expression using Boolean operators to provide flexible matching of communities. The AND operator provides functionality equivalent to the **community** *name* **members** command; the OR operator allows an OR match of communities; and the NOT operator allows inverted matches. If required, operators may be chained (for example, AND NOT) or enclosed within parentheses. The entire expression must be enclosed within quotation marks.

- **community** “north2” **expression** “target:1234:111 AND target:1234:222 AND target:1234:333”
- **community** “south” **expression** “target:1234:111 OR target:1234:222”
- **community** “east” **expression** “target:1234:1.1 AND NOT target:1234:191”
- **community** “west” **expression** “[community list A] OR ([community list B] AND [community list C])”

The first example above demonstrates the implementation of AND operators, which is equivalent to the **members** syntax (that is, “north” and “north2” are equivalent). The second example shows the OR operator, which will match a route that has target:1234:111 or target:1234:222. The third example shows the combined AND NOT operators, which will match a route that matches the regular expression for target:1234:1.1 except for target:1234.191, where “1.1” means any match of 111, 121, 131, 141, 151, 161, 171, 181, or 191. The fourth example shows the grouping of lists B and C through the use of parentheses.

The **no** form of the command deletes the community list or the provided community ID.

Default no community

Parameters *name* — the community list or expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

comm-id — the community ID. Up to 15 community ID strings can be specified with a total maximum of 72 characters. A community ID can be specified in four different forms:

- *2byte-asnumber*:*comm-val*
- *reg-ex*
- *ext-comm*
- *well-known-comm*

Values *2byte-asnumber*:*comm-val* — the *2byte-asnumber* is the Autonomous System Number (ASN) and *comm-val* is the community value, where:

2byte-asnumber: 0 to 65535

comm-val: 0 to 65535

reg-ex — a regular expression string. Allowed values are any string up to 72 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. See Regular Expressions for information.

ext-comm — the extended community, where *ext-comm* is defined as:

*type***:{***ip-address*:*comm-val* | *reg-ex1&reg-ex2* | *ip-address&reg-ex2* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*}, and where:

type: **target** or **origin** (keywords that denote the community as an extended community of type route target or route origin, respectively)

ip-address: a.b.c.d

comm-val: 0 to 65535

2byte-asnumber: 0 to 65535

ext-comm-val: 0 to 4294967295

4byte-asnumber: 0 to 4294967295

reg-ex1: a regular expression string, 63 characters maximum (see *reg-ex*, above)

reg-ex2: a regular expression string, 63 characters maximum (see *reg-ex*, above)

well-known-comm — one of the keywords **null**, **no-export**, **no-export-subconfed**, **no-advertise**

expression — a logical community expression containing terms and operators. It can contain sub-expressions enclosed in parentheses. Allowed values are any string up to 900 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.

Values *expression* is one of the following:

expression {AND | OR} *expression*

[NOT] (*expression*)

[NOT] *comm-id*

exact — the community expression only matches the route with the specified *expression*. Without the **exact** keyword, a community expression evaluates to be true if any member is present.

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 n/a

policy-statement

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

Context config>router>policy-options

Description This command enables 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

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.

triggered-policy

Syntax [**no**] **triggered-policy**

Context config>router

Description This command triggers route policy re-evaluation.

By default, when a change is made to a policy in the **config router policy-options** context and then committed, the change is effective immediately. However, there may be circumstances where the changes should or must be delayed; for example, when a policy change is implemented that would affect every BGP peer on a 7705 SAR. It is more effective to control changes on a peer-by-peer basis.

If the **triggered-policy** command is enabled and a given peer is established, and you want the peer to remain up, then, in order for a change to a route policy to take effect, a **clear** command with the **soft** or **soft-inbound** option must be used. In other words, when a **triggered-policy** is enabled, any routine policy change or policy assignment change within the protocol will not take effect until the protocol is reset or a **clear** command is issued to re-evaluate route policies; for example, **clear router bgp neighbor x.x.x.x soft**. This keeps the peer up, and the change made to a route policy is applied only to that peer, or group of peers.

Default disabled — dynamic route policy is enabled; policy-option configuration changes take effect immediately

7.9.2.1.3 Route Policy Damping Commands

damping

Syntax [**no**] **damping** *name*

Context config>router>policy-options

Description This command creates a context to configure a route damping profile to use in route policy entries.

If damping is enabled and the route policy does not specify a damping profile, the default damping profile is used. This default profile is always present and consists of the following parameters:

- Half-life: 15 m
- Max-suppress: 60 m
- Suppress-threshold: 3000
- Reuse-threshold: 750

The **no** form of the command deletes the named route damping profile and uses the default damping profile.

Default no damping

Parameters *name* — the damping profile name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

half-life

Syntax **half-life** *minutes*
no half-life

Context config>router>policy-options>damping

Description This command configures the half-life value for the route damping profile.

The half-life value is the time, expressed in minutes, required for a route to remain stable in order for the Figure of Merit (FoM) value to be reduced by one half; for example, if the half-life value is 6 and the route remains stable for 6 min, then the new FoM value is 3. After another 3 min pass and the route remains stable, the new FoM value is 1.5.

When the FoM value falls below the reuse threshold, the route is once again considered valid and can be reused or included in route advertisements.

The **no** form of the command removes the half-life parameter from the damping profile and uses the value from the default profile.

Default no half-life

Parameters *minutes* — the half-life in minutes, expressed as a decimal integer

Values 1 to 45

Default 15

max-suppress

Syntax **max-suppress** *minutes*
no max-suppress

Context config>router>policy-options>damping

Description This command configures the maximum suppression value for the route damping profile.

This value indicates the maximum time, expressed in minutes, that a route can remain suppressed.

The **no** form of the command removes the maximum suppression parameter from the damping profile and uses the value from the default profile.

Default no max-suppress

Parameters *minutes* — the maximum suppression time, in minutes, expressed as a decimal integer

Values 1 to 720

Default 60

reuse

Syntax **reuse** *integer*
no reuse

Context config>router>policy-options>damping

Description This command configures the reuse value for the route damping profile. This value must be less than the suppress value.

When the Figure of Merit (FoM) value falls below the reuse threshold, the route is once again considered valid and can be reused or included in route advertisements.

The **no** form of the command removes the reuse parameter from the damping profile and uses the value from the default profile.

Default no reuse

Parameters *integer* — the reuse value, expressed as a decimal integer

Values 1 to 20000

Default 750

suppress

Syntax **suppress** *integer*
no suppress

Context config>router>policy-options>damping

Description This command configures the suppression value for the route policy damping profile. This value must be greater than the reuse value

A route is suppressed when it has flapped frequently enough to increase the Figure of Merit (FoM) value so that it exceeds the suppress threshold limit. When the FoM value exceeds the suppress threshold limit, the route is removed from the route table or inclusion in advertisements.

The **no** form of the command removes the suppress parameter from the damping profile and uses the value from the default profile.

Default no suppress

Parameters *integer* — the suppress value expressed as a decimal integer

Values 1 to 20000

Default 3000

7.9.2.1.4 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.

An empty prefix list can be configured for preprovisioning. This empty prefix list will not find a match when referred to by a policy. When removing member prefixes from a prefix list, the prefix list will not automatically be removed when the last member is removed. If required, an empty prefix list must be explicitly removed using the **no** form of the command.

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

Default n/a

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-prefixIprefix-length* [**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/prefix-length* — the IPv4 or IPv6 prefix for the prefix list entry

Values	*ipv4-prefix*	a.b.c.d (host bits must be 0)
	ipv4-prefix-length	0 to 32
	ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x - [0 to FFFF]H d - [0 to 255]D
	ipv6-prefix-length	0 to 128

exact — the prefix list entry only matches the route with the specified *ip-prefix* and *prefix-length* values

longer — the prefix list entry matches any route that matches the specified *ip-prefix* and has a *prefix-length* value greater than the specified *prefix-length*

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

Values 0 to 128 (*length* > *prefix-length*)

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

Values 0 to 128 (*length*2 > *length1* > *prefix-length*)

7.9.2.1.5 Route Policy Entry Match Commands

entry

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

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

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

Multiple entries can be created using unique entries. The 7705 SAR 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 n/a

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 enables 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.

to

Syntax [**no**] **to**

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

Description This command enables the context to configure export policy match criteria based on a route's destination or the protocol into which the route is being advertised.

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

The **to** command context only applies to export policies. If it is used for an import policy, match criteria is ignored.

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

area

Syntax **area** *area-id*
no area

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

Description This command configures an OSPF area as a route policy match criterion.

This match criterion is only used in export policies.

All OSPF routes (internal and external) are matched using this criterion if the best path for the route is by the specified area.

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

Default n/a

Parameters *area-id* — the OSPF area ID expressed in dotted-decimal notation or as a 32-bit decimal integer

Values 0.0.0.0 to 255.255.255.255 (dotted-decimal), 0 to 4294967295 (decimal)

as-path

Syntax **as-path** *name*
no as-path

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

Description This command configures an AS path regular expression statement as a match criterion for the route policy entry. If no AS path criterion is specified, any AS path is considered to match. AS path regular expression statements are configured at the global route policy level (**config>router>policy-options>as-path** *name*).

The **no** form of the command removes the AS path regular expression statement as a match criterion.

Default no as-path

Parameters *name* — the AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The *name* specified must already be defined.

community

Syntax **community** *comm-name*
community expression *expression*
no community

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

Description This command configures a community list or expression as a match criterion for the route policy entry. If no community list or expression is specified, any community is considered a match.

The **no** form of the command removes the community list or expression match criterion.

Default no community

Parameters *comm-name* — the community list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The *comm-name* specified must already have its members defined using the **config>router>policy-options>community** *name* **members** command.

expression — the community expression. Allowed values are any expression up to 900 characters long composed of one or more expressions separated by AND, OR, and NOT operators. Operators may be combined (for example, OR NOT).

An expression can also be a community name enclosed in square brackets.

If the expression contains special characters (#, $, spaces, etc.), the entire string must be enclosed in double quotes.

The *expression* specified must already be defined using the **config>router>policy-options>community** *name* **expression** command.

Values *expression* is one of the following:
expression {AND | OR} *expression*
[NOT] (*expression*)
[NOT] "["*comm-name*"]"

external

Syntax [**no**] **external**

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

Description This command specifies the external IS-IS route matching criteria for the entry.

Default no external

family

Syntax **family** [**ipv4**] [**vpn-ipv4**] [**label-ipv4**] [**bgp-ls**]
no family

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

Description This command specifies address families as matching conditions.

Parameters **ipv4** — specifies IPv4 routing information

vpn-ipv4 — specifies VPN-IPv4 routing information

label-ipv4 — specifies labeled IPv4 routing information

bgp-ls — specifies BGP-LS routing information

group-address

Syntax **group-address** *prefix-list-name*
no group-address

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

Description This command specifies the multicast group address prefix list containing multicast group addresses that are embedded in the join or prune packet as a filter criterion. The prefix list must be configured prior to entering this command. Prefix lists are configured in the **config>router>policy-options>prefix-list** context.

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

Default no group-address

Parameters *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 *prefix-list-name* is defined in the **config>router>policy-options>prefix-list** context.

interface

Syntax **interface** *interface-name*
no interface

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

Description This command specifies the router interface, specified either by name or address, as a filter criterion.

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

Default no interface

Parameters *interface-name* — the name of the interface used as a match criterion for this entry. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

level

Syntax **level** {**1** | **2**}
no level

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

Description This command specifies the IS-IS route level as a match criterion for the entry.

Default no level

Parameters **1 | 2** — matches the IS-IS route learned from level 1 or level 2

neighbor

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

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

Description This command specifies the neighbor address as found in the source address of the actual join and prune message as a filter criterion. If no neighbor is specified, any neighbor is considered a match.

The **no** form of the command removes the neighbor IP match criterion from the configuration.

Default no neighbor

Parameters *ip-address* — the neighbor IPv4 or IPv6 address

Values	*ipv4-address*	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x[-interface]
		x:x:x:x:x:x:d.d.d.d[-interface]
		x - [0 to FFFF]H
		d - [0 to 255]D
		interface - 32 chars max, mandatory for link local addresses

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.

origin

Syntax **origin** {**igp** | **egp** | **incomplete** | **any**}
no origin

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

Description This command configures a BGP origin attribute as a match criterion for a route policy statement entry. If no origin attribute is specified, any BGP origin attribute is considered a match.

The **no** form of the command removes the BGP origin attribute match criterion.

Default no origin

Parameters **igp** — configures matching path information originating within the local AS

egp — configures matching path information originating in another AS

incomplete — configures matching path information learned by another method

any — ignores this criteria

prefix-list

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

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

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

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

An empty prefix list will evaluate as if no match was found.

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

Up to five prefix list names can be specified.

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

Default no prefix-list

Parameters *name* — the prefix list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

protocol

Syntax **protocol** *protocol* [**all** | {**instance** *instance*}]
protocol bgp bgp-label
no protocol

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

Description This command configures a routing protocol as a match criterion for a route policy statement entry. This command is used for both import and export policies depending on how it is used.

If no protocol criterion is specified, any protocol is considered a match.

The **no** form of the command removes all instances of the protocol from the match criterion.

Default no protocol

Parameters *protocol* — the protocol name to match. The list of protocols supported under **from** differs from the list supported under **to**.

Values Under **from**:

aggregate, bgp, bgp-vpn, direct, igmp, isis, ldp, managed, mld, nat, ospf, ospf3, pim, rip, static

Under **to**:

bgp, ospf, rip, isis, bgp-vpn, ospf3

all — specifies that all instances of the protocol are used as match criteria (only applies to IS-IS

instance — the instance ID of the specified protocol (only applies to IS-IS). If no *instance* is specified, instance 0 is used.

Values		
	isis-inst	0 to 31
	ospf-inst	0 to 31
	ospf3-inst	0 to 31

source-address

Syntax **source-address** *ip-address*
no source-address

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

Description This command specifies a multicast data source address or prefix list as a match criterion for this entry.

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

Default n/a

Parameters *ip-address* — the source IPv4 or IPv6 address

Values		
	ipv4-address	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0 to 255]D

tag

Syntax **tag** *tag*
no tag

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

Description This command adds an integer tag to the static or IGP routes. These tags are then matched to control route redistribution. A decimal or hexadecimal value can be entered. Values entered in hexadecimal are converted to decimal in the CLI.

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

Default no tag

Parameters *tag* — matches a specific external LSA tag field (can be hexadecimal or decimal)

Values

static, OSPF, and IS-IS:	[0x1...0xFFFFFFFF]H or 1 to 4294967295
RIP:	[0x1...0xFFFF]H or 1 to 65535

type

Syntax **type** *type*
no type

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

Description This command configures an OSPF type metric as a match criterion in the route policy statement entry.

If no type is specified, any OSPF type is considered a match.

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

Parameters *type* — the OSPF type metric

Values 1 — set as OSPF routes with type 1 LSAs
2 — set as OSPF routes with type 2 LSAs

7.9.2.1.6 Route Policy Action Commands

default-action

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

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

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

If a default action is defined and no matches occurred with the entries in the policy, the default action clause is used.

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

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

Default no default-action

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

next-entry — the actions specified will be made to the route attributes and then policy evaluation will continue with the next policy entry (if any others are specified)

next-policy — the actions specified will be made to the route attributes and then policy evaluation will continue with the next route policy (if any others are specified)

reject — routes matching the entry match criteria will be rejected

action

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

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

Description This command enables 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 — the actions specified will be made to the route attributes and then policy evaluation will continue with the next policy entry (if any others are specified)

next-policy — the actions specified will be made to the route attributes and then policy evaluation will continue with the next route policy (if any others are specified)

reject — routes matching the entry match criteria will be rejected

aigp-metric

Syntax **aigp-metric** *metric*
aigp-metric *metric* **add**
aigp-metric igp
no aigp-metric

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

Description This command assigns a BGP AIGP metric to routes matching the entry. The effect of this command on a route that is matched and accepted by a route policy entry depends on how the policy is applied (whether it is a BGP import policy or BGP export policy), the type of route, and the specific form of the command.

In a BGP import policy, this command is used to:

- associate an AIGP metric with an IBGP route received with an empty AS path and no AIGP attribute
- associate an AIGP metric with an EBGP route received without an AIGP attribute that has an AS path containing only AS numbers belonging to the local AIGP administrative domain
- modify the received AIGP metric value prior to BGP path selection

In a BGP export policy, this command is used to:

- add the AIGP attribute and set the AIGP metric value in a BGP route originated by exporting a direct, static, or IGP route from the routing table
- remove the AIGP attribute from a route advertisement to a particular peer
- modify the AIGP metric value in a route advertisement to a particular peer

The **no** form of the command removes the AIGP metric from the routes.

Default no aigp-metric

Parameters *metric* — the administratively defined metric

Values 0 to 4294967295

metric **add** — adds a configured metric value to the current AIGP metric value

Values 0 to 4294967295

igp — sets the AIGP metric value to the IGP metric value

as-path

Syntax **as-path** {**add** | **replace**} *name*
no as-path

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

Description This command assigns a BGP AS path list to routes matching the route policy statement entry. If no AS path list is specified, the AS path attribute is not changed.

The **no** form of the command disables the AS path list editing action from the route policy entry.

Default no as-path

Parameters **add** — the AS path list is to be prepended to an existing AS list

replace — the AS path list replaces any existing AS path attribute

name — the AS path list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. The name specified must already be defined.

as-path-prepend

Syntax **as-path-prepend** *as-number* [*repeat*]
no as-path-prepend

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

Description This command prepends a BGP AS number once or numerous times to the AS path attribute of routes matching the route policy statement entry. If an AS number is not configured, the AS path is not changed.

If the optional number is specified, then the AS number is prepended as many times as indicated by the number.

The **no** form of the command disables the AS path prepend action from the route policy entry.

Default no as-path-prepend

Parameters *as-number* — the AS number to prepend expressed as a decimal integer

Values 1 to 4294967295

repeat — the number of times to prepend the specified AS number expressed as a decimal integer

Values 1 to 50

community

Syntax **community add** *name* [*name*...(up to 28 max)]
community remove *name* [*name*...(up to 28 max)]
community replace *name* [*name*...(up to 28 max)]
no community

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

Description This command adds, removes, or replaces a BGP community list or expression to or from routes matching the route policy statement entry. If no community list or expression is specified, the community path attribute is not changed. Up to 28 community list or expression names can be used in one add, remove, or replace command.

The community list or expression changes the community path attribute according to the **add**, **remove** or **replace** keywords. If more than one of the keywords is used in a single command, first **add** is applied, then **remove** is applied. However, **replace** overwrites any **add** or **remove**.

The **no** form of the command disables the action to edit the community path attribute for the route policy entry.

Default no community

Parameters **add** — the specified community list or expression is added to any existing list of communities

remove — the specified community list or expression is removed from the existing list of communities

replace — the specified community list or expression replaces any existing community attribute

name — the community list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

damping

Syntax **damping** {*name* | **none**}
no damping

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

Description This command configures a damping profile used for routes matching the route policy statement entry. If no damping criteria is specified, the default damping profile is used.

The **no** form of the command removes the damping profile associated with the route policy entry.

Default no damping

Parameters *name* — the damping profile name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. The name specified must already be defined.

none — disables route damping for the route policy

local-preference

Syntax **local-preference** *local-preference*
no local-preference

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

Description This command assigns a BGP local preference to routes matching a route policy statement entry. If no local preference is specified, the BGP configured local preference is used.

The **no** form of the command disables assigning a local preference in the route policy entry.

Default no local-preference

Parameters *local-preference* — the local preference expressed as a decimal integer

Values 0 to 4294967295

metric

Syntax **metric** {**add** | **subtract**} *metric*
metric set {**igp** | *metric*}
no metric

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

Description In a BGP import or export policy, this command assigns a Multi-Exit Discriminator (MED) value to routes matched by the policy statement entry. The MED value may be set to a fixed value (overriding the received value), set to the routing table cost of the route that is used to resolve the next hop of the BGP route (the **metric set igp** command), or modified by adding or subtracting a fixed value offset (the **metric add | subtract** command).

When used in a BGP export policy, the **metric set igp** command has the same effect as the **med-out igp-cost** command (see the 7705 SAR Routing Protocols Guide, “BGP Command Reference”) except that it applies only to the routes matched by the policy entry. The effect of the **metric set igp** command depends on the BGP policy type and the route type as summarized in Table 123.

Table 123 **Effect of Setting the metric set igp Command**

BGP Policy Type	Matched Route Type	Effect of metric set igp Command
Export	Non-BGP route (for example, static, OSPF, or IS-IS)	Adds the MED attribute and sets it to the metric of the non-BGP route in the routing table manager (RTM)
Export	BGP route without MED	Adds the MED attribute and sets it to the metric of the route or tunnel used to resolve the BGP next hop
Export	BGP route with MED assigned	Overwrites the MED value with the metric of the route or tunnel used to resolve the BGP next hop

The **no** form of the command removes the MED value from the route policy statement. If a MED value is configured for a BGP peer using the **med-out** command, that value is used (see the 7705 SAR Routing Protocols Guide, “BGP Command Reference”). If no MED is configured, no MED value is advertised.

Default no metric

Parameters **add** — the specified *metric* is added to any existing metric. If the result of the addition results in a number greater than 4294967295, the value 4294967295 is used.

subtract — the specified *metric* is subtracted from any existing metric. If the result of the subtraction results in a number less than 0, the value of 0 is used.

set — the specified *metric* replaces any existing metric

igp — sets the MED value to the routing table cost of the route that is used to resolve the next hop of the BGP route

metric — the metric modifier expressed as a decimal integer

Values 0 to 4294967295

next-hop

Syntax **next-hop** *ip-address*
no next-hop

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

Description This command assigns the specified next-hop IP address to routes matching the policy statement entry. If a next-hop IP address is not specified, the next-hop attribute is not changed.

The **no** form of the command disables assigning a next-hop address in the route policy entry.

Default no next-hop

Parameters *ip-address* — the next-hop IP address

Values	*ipv4-address*	a.b.c.d
	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x - [0 to FFFF]H
		d - [0 to 255]D

next-hop-self

Syntax [**no**] **next-hop-self**

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

Description This command advertises a next-hop IP address belonging to this router even if a third-party next hop is available to routes matching the policy statement entry.

The **no** form of the command disables advertising the next-hop-self option for the route policy entry.

Default no next-hop-self

origin

Syntax **origin** {**igp** | **egp** | **incomplete**}
no origin

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

Description This command sets the BGP origin assigned to routes exported into BGP.

If the routes are exported into protocols other than BGP, this option is ignored.

The **no** form of the command disables setting the BGP origin for the route policy entry.

Default no origin

Parameters **igp** — sets the path information as originating within the local AS

egp — sets the path information as originating in another AS

incomplete — sets the path information as learned by some other means

preference

Syntax **preference** *preference*
no preference

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

Description This command assigns a route preference to routes matching the route policy statement entry.

If no preference is specified, the default route table manager (RTM) preference for the protocol is used.

The **no** form of the command disables setting an RTM preference in the route policy entry.

Default no preference

Parameters *preference* — the route preference expressed as a decimal integer

Values 1 to 255 (0 represents unset, MIB only)

tag

Syntax **tag** *tag*
no tag

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

Description This command assigns an OSPF, IS-IS, or RIP tag to routes that do not match any entry (for default action) or that match the entry (for action). A decimal or hexadecimal value can be entered. Values entered in hexadecimal are converted to decimal in the CLI.

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

Default no tag

Parameters *tag* — assigns an OSPF, IS-IS, or RIP tag (decimal or hexadecimal values)

Values

OSPF and IS-IS:	[0x1...0xFFFFFFFF]H or 1 to 4294967295
RIP:	[0x1...0xFFFF]H or 1 to 65535

type

Syntax **type** *type*
no type

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

Description This command assigns an OSPF type metric to routes that do not match any entry (for default action) or that match the entry (for action). The **no** form of the command disables assigning an OSPF type in the route policy entry.

Default no type

Parameters *type* — specifies the OSPF type metric

Values 1 — set as OSPF routes with type 1 LSAs
2 — set as OSPF routes with type 2 LSAs

7.9.2.2 Show Commands

Note: The following command outputs are examples only; actual displays may differ depending on supported functionality and user configuration.

policy

Syntax **policy** [*name* | **damping** *name* | **prefix-list** *name* |**as-path** *name* | **community** *name* | **admin**]

Context show>router

Description This command displays configured policy statement information.

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

damping — displays the damping profile for use in the route policy

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

as-path — displays AS path regular expression statements used in the route policy

community — displays community lists used in the route policy

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

Output The following outputs are examples of route policy information, and Table 124 describes the fields.

- Output Example - show router policy
- Output Example - show router policy admin
- Output Example - show router policy name
- Output Example - show router policy damping
- Output Example - show router policy prefix-list
- Output Example - show router policy prefix-list name
- Output Example - show router policy as-path
- Output Example - show router policy as-path name
- Output Example - show router policy community
- Output Example - show router policy community name

Output Example - show router policy

The **show router policy** command displays all configured route policies.

```
A:ALU-1# show router policy
===============================================================================
Route Policies
===============================================================================
Policy                          Description
-------------------------------------------------------------------------------
BGP To OSPF                      Policy Statement For 'BGP To OSPF'
Direct And Aggregate            Policy Statement ABC
-------------------------------------------------------------------------------
Policies : 3
===============================================================================
A:ALU-1#
```

Output Example - show router policy admin

The **show router policy admin** command is similar to the info command, which displays information about the route policies and parameters.

```
A:ALU-1# show router policy admin
    prefix-list "All-Routes"
    prefix 0.0.0.0/0 longer
    prefix 2.0.0.0/8 longer
    prefix 3.0.0.0/8 longer
    prefix 4.0.0.0/8 longer
    prefix 5.0.0.0/8 longer
    prefix 6.0.0.0/8 exact
    prefix 224.0.0.0/24 longer
   exit
   community "65206" members "no-export" "no-export-subconfed"
   community "AS65000" members "701:65000"
   as-path "test" "14001 701"
   as-path "test1" "1234{1,6} (56|47) (45001|2000|1534)* 9+"
   damping "TEST-LOW"
    half-life 22
    max-suppress 720
    reuse 10000
    suppress 15000
   exit
   damping "TEST-HIGH"
    half-life 22
    max-suppress 720
    reuse 1000
    suppress 5000
   exit
   damping "TEST-MEDIUM"
    half-life 22
    max-suppress 720
    reuse 5000
    suppress 11000
   exit
   policy-statement "BGP To OSPF"
    description "Policy Statement For 'BGP To OSPF'"
    entry 10
        description "Entry For Policy 'BGP To OSPF"
        from
```

```
            protocol bgp
        exit
        to
            protocol rip
        exit
        action accept
            metric set 1
            next-hop 10.0.18.200
            tag 134250805
        exit
    exit
    default-action reject
    exit
    policy-statement "Direct And Aggregate"
        entry 10
            from
                protocol direct
            exit
            to
                protocol bgp
                exit
                action accept
                exit
            exit
            entry 20
            from
                protocol aggregate
            exit
            to
                protocol bgp
            exit
            action accept
            exit
        exit
    exit
...
A:ALU-1#
```

Output Example - show router policy name

The **show router policy** *name* command displays information about a specific route policy.

```
description "Policy Statement For 'BGP To OSPF'"
    entry 10
     description "Entry For Policy 'BGP To OSPF"
     from
      protocol bgp
     exit
     to
      protocol rip
     exit
     action accept
      metric set 1
      next-hop 10.0.18.200
      tag 134250805
     exit
    exit
    default-action reject
A:ALU-1#
```

Output Example - show router policy damping

The **show router policy damping** command displays information about the route policy damping configurations.

```
A:ALU-1# show router policy damping
===============================================
Route Damping Profiles
===============================================
    damping "TEST-LOW"
     half-life 22
     max-suppress 720
     reuse 10000
     suppress 15000
    exit
    damping "TEST-HIGH"
     half-life 22
     max-suppress 720
     reuse 1000
     suppress 5000
    exit
    damping "TEST-MEDIUM"
     half-life 22
     max-suppress 720
     reuse 5000
     suppress 11000
    exit
===============================================
A:ALU-1#
```

Output Example - show router policy prefix-list

The **show router policy prefix-list** command displays a list of configured prefix lists.

```
A:ALU-1# show router policy prefix-list
==================================
Prefix Lists
==================================
Prefix List Name
----------------------------------
All-Routes
==================================
A:ALU-1#
```

Output Example - show router policy prefix-list name

The show **router policy prefix-list** *name* command displays information about a specific prefix list.

```
A:ALU-1# show router policy prefix-list All-Routes
    prefix 0.0.0.0/0 longer
    prefix 2.0.0.0/8 longer
    prefix 3.0.0.0/8 longer
    prefix 4.0.0.0/8 longer
    prefix 5.0.0.0/8 longer
    prefix 6.0.0.0/8 exact
    prefix 224.0.0.0/24 longer
A:ALU-1#
```

Output Example - show router policy as-path

The **show router policy as-path** command displays a list of configured AS paths.

```
A:ALU-1# show router policy as-path
==================================
AS Paths
==================================
AS Path Name
----------------------------------
test
test1
----------------------------------
AS Paths : 2
==================================
A:ALU-1#
```

Output Example - show router policy as-path name

The **show router policy as-path** *name* command displays information about a specific AS path.

```
A:ALU-1# show router policy as-path test
as-path "test" "14001 701"
```

Output Example - show router policy community

The **show router policy community** command displays a list of configured communities.

```
A:ALU-1# show router policy community
==================================
Communities
==================================
Community Name
----------------------------------
65206
AS701
AS65000
----------------------------------
Communities : 3
==================================
A:ALU-1#
```

Output Example - show router policy community name

The **show router policy community** *name* command displays information about a specific community.

```
A:ALU-1# show router policy community 65206
community "65206" members "no-export" "no-export-subconfed"
A:ALU-1#
```

Table 124 **Route Policy Field Descriptions**

Label	Description
Policy	The list of route policy names
Description	The description of each route policy
Policies	The total number of policies configured
Damping Name	The damping profile name
half-life	The half-life parameter for the route damping profile
max-suppress	The maximum suppression value configured for the route damping profile
reuse	The reuse value configured for the route damping profile
suppress	The suppression value configured for the route damping profile
Prefix List Name	The prefix list name and IP address/mask and whether the prefix list entry only matches (exact) the route with the specified ip-prefix and prefix mask (length) values or values greater (longer) than the specified mask
AS Path Name	The list of AS path names
AS Paths	The total number of AS paths configured
Community Name	The list of community names
Communities	The total number of communities configured

8 List of Acronyms

Table 125 **Acronyms**

Acronym	Expansion
2G	second-generation wireless telephone technology
3DES	triple DES (data encryption standard)
3G	third-generation mobile telephone technology
6VPE	IPv6 on Virtual Private Edge Router
7705 SAR	7705 Service Aggregation Router
7750 SR	7750 Service Router
8 PSK	eight phase shift keying
16 QAM	16-state quadrature amplitude modulation
32 QAM	32-state quadrature amplitude modulation
64 QAM	64-state quadrature amplitude modulation
128 QAM	128-state quadrature amplitude modulation
256 QAM	256-state quadrature amplitude modulation
ABR	area border router available bit rate
AC	alternating current attachment circuit
ACK	acknowledge
ACL	access control list
ACR	adaptive clock recovery
AD	auto-discovery
ADM	add/drop multiplexer
ADP	automatic discovery protocol
AES	advanced encryption standard
AFI	authority and format identifier
AIGP	accumulated IGP
AIS	alarm indication signal

Table 125 **Acronyms (Continued)**

Acronym	Expansion
ALG	application level gateway
ANSI	American National Standards Institute
Apipe	ATM VLL
APS	automatic protection switching
ARP	address resolution protocol
A/S	active/standby
AS	autonomous system
ASAP	any service, any port
ASBR	autonomous system boundary router
ASM	any-source multicast autonomous system message
ASN	autonomous system number
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit
AU	administrative unit
AUG	administrative unit group
B3ZS	bipolar with three-zero substitution
Batt A	battery A
B-bit	beginning bit (first packet of a fragment)
BBE	background block errors
Bc	committed burst size
Be	excess burst size
BECN	backward explicit congestion notification
Bellcore	Bell Communications Research
BFD	bidirectional forwarding detection
BGP	border gateway protocol
BGP-LS	border gateway protocol link state
BGP-LU	border gateway protocol labeled unicast

Table 125 **Acronyms (Continued)**

Acronym	Expansion
BITS	building integrated timing supply
BMCA	best master clock algorithm
BMU	broadcast, multicast, and unknown traffic Traffic that is not unicast. Any nature of multipoint traffic: • broadcast (that is, all 1s as the destination IP to represent all destinations within the subnet) • multicast (that is, traffic typically identified by the destination address, uses special destination address); for IP, the destination must be 224.0.0.0 to 239.255.255.255 • unknown (that is, the destination is typically a valid unicast address but the destination port/interface is not yet known; therefore, traffic needs to be forwarded to all destinations; unknown traffic is treated as broadcast)
BNM	bandwidth notification message
BOF	boot options file
BoS	bottom of stack
BPDU	bridge protocol data unit
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSM	bootstrap message
BSR	bootstrap router
BSTA	Broadband Service Termination Architecture
BTS	base transceiver station
CA	certificate authority
CAS	channel associated signaling
CBN	common bonding networks
CBS	committed buffer space
CC	continuity check control channel
CCM	continuity check message
CCTV	closed-circuit television

Table 125 **Acronyms (Continued)**

Acronym	Expansion
CE	circuit emulation customer edge
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
CFM	connectivity fault management
cHDLC	Cisco high-level data link control protocol
CIDR	classless inter-domain routing
CIR	committed information rate
CLI	command line interface
CLP	cell loss priority
CMP	certificate management protocol
C-multicast	customer multicast
CoS	class of service
CPE	customer premises equipment
Cpipe	circuit emulation (or TDM) VLL
CPM	Control and Processing Module (CPM is used instead of CSM when referring to CSM filtering to align with CLI syntax used with other SR products). CSM management ports are referred to as CPM management ports in the CLI.
CPROTO	C prototype
CPU	central processing unit
C/R	command/response
CRC	cyclic redundancy check
CRC-32	32-bit cyclic redundancy check
CRL	certificate revocation list
CRON	a time-based scheduling service (from chronos = time)
CRP	candidate RP
CSM	Control and Switching Module

Table 125 **Acronyms (Continued)**

Acronym	Expansion
CSNP	complete sequence number PDU
CSPF	constrained shortest path first
C-TAG	customer VLAN tag
CV	connection verification customer VLAN (tag)
CW	control word
CWDM	coarse wavelength-division multiplexing
DA/FAN	distribution automation and field area network
DC	direct current
DC-C	DC return - common
DCE	data communications equipment
DC-I	DC return - isolated
DCO	digitally controlled oscillator
DCR	differential clock recovery
DDoS	distributed DoS
DE	discard eligibility
DER	distinguished encoding rules
DES	data encryption standard
DF	do not fragment designated forwarder
DH	Diffie-Hellman
DHB	decimal, hexadecimal, or binary
DHCP	dynamic host configuration protocol
DHCPv6	dynamic host configuration protocol for IPv6
DIS	designated intermediate system
DLCI	data link connection identifier
DLCMI	data link connection management interface
DM	delay measurement

Table 125 **Acronyms (Continued)**

Acronym	Expansion
DNS	domain name server
DNU	do not use
DoS	denial of service
dot1p	IEEE 802.1p bits, in Ethernet or VLAN ingress packet headers, used to map traffic to up to eight forwarding classes
dot1q	IEEE 802.1q encapsulation for Ethernet interfaces
DPD	dead peer detection
DPI	deep packet inspection
DPLL	digital phase locked loop
DR	designated router
DSA	digital signal algorithm
DSCP	differentiated services code point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
DTE	data termination equipment
DU	downstream unsolicited
DUID	DHCP unique identifier
DUS	do not use for synchronization
DV	delay variation
DVMRP	distance vector multicast routing protocol
e911	enhanced 911 service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
E-bit	ending bit (last packet of a fragment)
E-BSR	elected BSR
ECMP	equal cost multipath
EE	end entity
EFM	Ethernet in the first mile

Table 125 **Acronyms (Continued)**

Acronym	Expansion
EGP	exterior gateway protocol
EIA/TIA-232	Electronic Industries Alliance/Telecommunications Industry Association Standard 232 (also known as RS-232)
EIR	excess information rate
EJBCA	Enterprise Java Bean Certificate Authority
E-LAN	Ethernet local area network
E-Line	Ethernet virtual private line
EL	entropy label
eLER	egress label edge router
ELI	entropy label indicator
E&M	ear and mouth earth and magneto exchange and multiplexer
eMBMS	evolved MBMS
EOP	end of packet
EPC	evolved packet core
EPD	early packet discard
Epipe	Ethernet VLL
EPL	Ethernet private line
EPON	Ethernet Passive Optical Network
EPS	equipment protection switching
ERO	explicit route object
ES	Ethernet segment errored seconds
ESD	electrostatic discharge
ESI	Ethernet segment identifier
ESMC	Ethernet synchronization message channel
ESN	extended sequence number
ESP	encapsulating security payload

Table 125 **Acronyms (Continued)**

Acronym	Expansion
ESPI	encapsulating security payload identifier
ETE	end-to-end
ETH-BN	Ethernet bandwidth notification
ETH-CFM	Ethernet connectivity fault management (IEEE 802.1ag)
EVC	Ethernet virtual connection
EVDO	evolution - data optimized
EVI	EVPN instance
EVPL	Ethernet virtual private link
EVPN	Ethernet virtual private network
EXP bits	experimental bits (currently known as TC)
FC	forwarding class
FCS	frame check sequence
FD	frequency diversity
FDB	forwarding database
FDL	facilities data link
FEAC	far-end alarm and control
FEC	forwarding equivalence class
FECN	forward explicit congestion notification
FeGW	far-end gateway
FEP	front-end processor
FF	fixed filter
FFD	fast fault detection
FIB	forwarding information base
FIFO	first in, first out
FIPS-140-2	Federal Information Processing Standard publication 140-2
FNG	fault notification generator
FOM	figure of merit

Table 125 **Acronyms (Continued)**

Acronym	Expansion
Fpipe	frame relay VLL
FQDN	fully qualified domain name
FR	frame relay
FRG bit	fragmentation bit
FRR	fast reroute
FTN	FEC-to-NHLFE
FTP	file transfer protocol
FXO	foreign exchange office
FXS	foreign exchange subscriber
GFP	generic framing procedure
GigE	Gigabit Ethernet
GLONASS	Global Navigation Satellite System (Russia)
GNSS	global navigation satellite system (generic)
GPON	Gigabit Passive Optical Network
GPRS	general packet radio service
GPS	Global Positioning System
GRE	generic routing encapsulation
GRT	global routing table
GSM	Global System for Mobile Communications (2G)
GTP-U	GPRS tunneling protocol user plane
GW	gateway
HA	high availability
HCM	high capacity multiplexing
HDB3	high density bipolar of order 3
HDLC	high-level data link control protocol
HEC	header error control
HMAC	hash message authentication code

Table 125 **Acronyms (Continued)**

Acronym	Expansion
Hpipe	HDLC VLL
H-QoS	hierarchical quality of service
HSB	hot standby
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
H-VPLS	hierarchical virtual private line service
IANA	internet assigned numbers authority
IBN	isolated bonding networks
ICB	inter-chassis backup
ICMP	Internet control message protocol
ICMPv6	Internet control message protocol for IPv6
ICP	IMA control protocol cells
IDS	intrusion detection system
IDU	indoor unit
IED	intelligent end device
IEEE	Institute of Electrical and Electronics Engineers
IEEE 1588v2	Institute of Electrical and Electronics Engineers standard 1588-2008
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force
IGMP	Internet group management protocol
IGP	interior gateway protocol
IID	instance ID
IKE	Internet key exchange
iLER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IMET-IR	inclusive multicast Ethernet tag—ingress replication

Table 125 **Acronyms (Continued)**

Acronym	Expansion
INVARP	inverse address resolution protocol
IOM	input/output module
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPIP	IP in IP
Ipipe	IP interworking VLL
I-PMSI	inclusive PMSI
IPoATM	IP over ATM
IPS	intrusion prevention system
IPSec	Internet Protocol security
IR	ingress replication
IRB	integrated routing and bridging
ISA	integrated services adapter
ISAKMP	Internet security association and key management protocol
IS-IS	Intermediate System-to-Intermediate System
IS-IS-TE	IS-IS-traffic engineering (extensions)
ISO	International Organization for Standardization
IW	interworking
JP	join prune
KG	key group
LB	loopback
lbf-in	pound force inch
LBM	loopback message
LBO	line buildout
LBR	loopback reply
LCP	link control protocol
LDP	label distribution protocol

Table 125 **Acronyms (Continued)**

Acronym	Expansion
LER	label edge router
LFA	loop-free alternate
LFIB	label forwarding information base
LIB	label information base
LLDP	link layer discovery protocol
LLDPDU	link layer discovery protocol data unit
LLF	link loss forwarding
LLID	loopback location ID
LM	loss measurement
LMI	local management interface
LOS	line-of-sight loss of signal
LSA	link-state advertisement
LSDB	link-state database
LSP	label switched path link-state PDU (for IS-IS)
LSPA	LSP attributes
LSR	label switch router link-state request
LSU	link-state update
LT	linktrace
LTE	long term evolution line termination equipment
LTM	linktrace message
LTN	LSP ID to NHLFE
LTR	link trace reply
MA	maintenance association
MAC	media access control
MA-ID	maintenance association identifier

Table 125 **Acronyms (Continued)**

Acronym	Expansion
MBB	make-before-break
MBGP	multicast BGP multiprotocol BGP multiprotocol extensions for BGP
MBMS	multimedia broadcast multicast service
MBS	maximum buffer space maximum burst size media buffer space
MBSP	mobile backhaul service provider
MCAC	multicast connection admission control
MC-APS	multi-chassis automatic protection switching
MC-MLPPP	multi-class multilink point-to-point protocol
MCS	multicast server multi-chassis synchronization
MCT	MPT craft terminal
MD	maintenance domain
MD5	message digest version 5 (algorithm)
MDA	media dependent adapter
MDDB	multidrop data bridge
MDL	maintenance data link
MDT	multicast distribution tree
ME	maintenance entity
MED	multi-exit discriminator
MEF	Metro Ethernet Forum
MEG	maintenance entity group
MEG-ID	maintenance entity group identifier
MEN	Metro Ethernet network
MEP	maintenance association end point
MFC	multi-field classification

Table 125 **Acronyms (Continued)**

Acronym	Expansion
MHD	multi-homed device
MHF	MIP half function
MHN	multi-homed network
MIB	management information base
MI-IS-IS	multi-instance IS-IS
MIR	minimum information rate
MLD	multicast listener discovery
mLDP	multicast LDP
MLPPP	multilink point-to-point protocol
mLSP	multicast LSP
MoFRR	multicast-only fast reroute
MP	merge point multilink protocol multipoint
MP-BGP	multiprotocol border gateway protocol
MPLS	multiprotocol label switching
MPLSCP	multiprotocol label switching control protocol
MPP	MPT protection protocol
MPR	see Wavence
MPR-e	Microwave Packet Radio (standalone mode)
MPT-HC V2/9558HC	Microwave Packet Transport, High Capacity version 2
MPT-HLC	Microwave Packet Transport, High-Capacity Long-Haul Cubic (ANSI)
MPT-HQAM	Microwave Packet Transport, High Capacity (MPT-HC-QAM) or Extended Power (MPT-XP-QAM) with 512/1024 QAM
MPT-MC	Microwave Packet Transport, Medium Capacity
MPT-XP	Microwave Packet Transport, High Capacity (very high power version of MPT-HC V2/9558HC)
MRAI	minimum route advertisement interval

Table 125 **Acronyms (Continued)**

Acronym	Expansion
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MSDP	Multicast Source Discovery Protocol
MSDU	MAC Service Data Unit
MSO	multi-system operator
MS-PW	multi-segment pseudowire
MSS	maximum segment size Microwave Service Switch
MTIE	maximum time interval error
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit
M-VPLS	management virtual private line service
MVPN	multicast VPN
MVR	multicast VPLS registration
MW	microwave
MWA	microwave awareness
N·m	newton meter
NAT	network address translation
NAT-T	network address translation traversal
NBMA	non-broadcast multiple access (network)
ND	neighbor discovery
NE	network element
NET	network entity title
NFM-P	Network Functions Manager - Packet (formerly 5620 SAM)
NGE	network group encryption
NG-MVPN	next generation MVPN
NH	next hop

Table 125 **Acronyms (Continued)**

Acronym	Expansion
NHLFE	next hop label forwarding entry
NHOP	next-hop
NLOS	non-line-of-sight
NLPID	network level protocol identifier
NLRI	network layer reachability information
NNHOP	next next-hop
NNI	network-to-network interface
Node B	similar to BTS but used in 3G networks — term is used in UMTS (3G systems) while BTS is used in GSM (2G systems)
NOC	network operations center
NPAT	network port address translation
NRC-F	Network Resource Controller - Flow
NRC-P	Network Resource Controller - Packet
NRC-T	Network Resource Controller - Transport
NRC-X	Network Resource Controller - Cross Domain
NSAP	network service access point
NSD	Network Services Director
NSP	native service processing Network Services Platform
NSSA	not-so-stubby area
NTP	network time protocol
NTR	network timing reference
OADM	optical add/drop multiplexer
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OC3	optical carrier level 3
OCSP	online certificate status protocol
ODU	outdoor unit

Table 125 **Acronyms (Continued)**

Acronym	Expansion
OIF	outgoing interface
OLT	optical line termination
OMC	optical management console
ONT	optical network terminal
OOB	out-of-band
OPX	off premises extension
ORF	outbound route filtering
OS	operating system
OSI	Open Systems Interconnection (reference model)
OSINLCP	OSI Network Layer Control Protocol
OSPF	open shortest path first
OSPF-TE	OSPF-traffic engineering (extensions)
OSS	operations support system
OSSP	organization specific slow protocol
OTP	one time password
OWAMP	one-way active measurement protocol
P2MP	point to multipoint
PADI	PPPoE active discovery initiation
PADR	PPPoE active discovery request
PAE	port authentication entities
PSB	path state block
PBO	packet byte offset
PBR	policy-based routing
PBX	private branch exchange
PCAP	packet capture
PCC	Path Computation Element Client
PCE	Path Computation Element

Table 125 **Acronyms (Continued)**

Acronym	Expansion
PCEP	Path Computation Element Protocol
PCM	pulse code modulation
PCP	priority code point
PCR	proprietary clock recovery
PDU	power distribution unit protocol data units
PDV	packet delay variation
PDVT	packet delay variation tolerance
PE	provider edge router
PEAPv0	protected extensible authentication protocol version 0
PEM	privacy enhanced mail
PFoE	power feed over Ethernet
PFS	perfect forward secrecy
PHB	per-hop behavior
PHP	penultimate hop popping
PHY	physical layer
PIC	prefix independent convergence
PID	protocol ID
PIM SSM	protocol independent multicast—source-specific multicast
PIR	peak information rate
PKCS	public key cryptography standards
PKI	public key infrastructure
PLAR	private line automatic ringdown
PLCP	Physical Layer Convergence Protocol
PLR	point of local repair
PLSP	path LSP
PMSI	P-multicast service interface
P-multicast	provider multicast

Table 125 **Acronyms (Continued)**

Acronym	Expansion
PoE	power over Ethernet
PoE+	power over Ethernet plus
POH	path overhead
POI	purge originator identification
PoP	point of presence
POS	packet over SONET
PPP	point-to-point protocol
PPPoE	point-to-point protocol over Ethernet
PPS	pulses per second
PRC	primary reference clock
PRS	primary reference source
PRTC	primary reference time clock
PSE	power sourcing equipment
PSK	pre-shared key
PSN	packet switched network
PSNP	partial sequence number PDU
PTA	PMSI tunnel attribute
PTM	packet transfer mode
PTP	performance transparency protocol precision time protocol
PuTTY	an open-source terminal emulator, serial console, and network file transfer application
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE	pseudowire emulation
PWE3	pseudowire emulation edge-to-edge
Q.922	ITU-T Q-series Specification 922

Table 125 **Acronyms (Continued)**

Acronym	Expansion
QL	quality level
QoS	quality of service
QPSK	quadrature phase shift keying
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RBS	robbed bit signaling
RD	route distinguisher
RDI	remote defect indication
RED	random early discard
RESV	reservation
RIB	routing information base
RIP	routing information protocol
RJ-45	registered jack 45
RMON	remote network monitoring
RNC	Radio Network Controller
RP	rendezvous point
RPF RTM	reverse path forwarding RTM
RPS	radio protection switching
RPT	rendezvous-point tree
RR	route reflector
RRO	record route object
RS-232	Recommended Standard 232 (also known as EIA/TIA-232)
RSA	Rivest, Shamir, and Adleman (authors of the RSA encryption algorithm)
RSHG	residential split horizon group
RSTP	rapid spanning tree protocol
RSVP-TE	resource reservation protocol - traffic engineering
RT	receive/transmit

Table 125 **Acronyms (Continued)**

Acronym	Expansion
RTC	route target constraint
RTM	routing table manager
RTN	battery return
RTP	real-time protocol
R&TTE	Radio and Telecommunications Terminal Equipment
RTU	remote terminal unit
RU	rack unit
r-VPLS	routed virtual private LAN service
SA	security association source-active
SAA	service assurance agent
SAFI	subsequent address family identifier
SAP	service access point
SAToP	structure-agnostic TDM over packet
SCADA	surveillance, control and data acquisition
SC-APS	single-chassis automatic protection switching
SCP	secure copy
SCTP	Stream Control Transmission Protocol
SD	signal degrade space diversity
SDH	synchronous digital hierarchy
SDI	serial data interface
SDN	software defined network
SDP	service destination point
SE	shared explicit
SeGW	secure gateway
SES	severely errored seconds
SETS	synchronous equipment timing source

Table 125 **Acronyms (Continued)**

Acronym	Expansion
SF	signal fail
SFP	small form-factor pluggable (transceiver)
SFTP	SSH file transfer protocol
(S,G)	(source, group)
SGT	self-generated traffic
SHA-1	secure hash algorithm
SHG	split horizon group
SIR	sustained information rate
SLA	Service Level Agreement
SLARP	serial line address resolution protocol
SLID	subscriber location identifier of a GPON module
SLM	synthetic loss measurement
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SNR	signal to noise ratio
SNTP	simple network time protocol
SONET	synchronous optical networking
S-PE	switching provider edge router
SPF	shortest path first
SPI	security parameter index
S-PMSI	selective PMSI
SPT	shortest path tree
SR	service router (7750 SR) segment routing
SRLG	shared risk link group
SRP	stateful request parameter
SRRP	subscriber routed redundancy protocol
SR-ISIS	segment routing IS-IS

Table 125 **Acronyms (Continued)**

Acronym	Expansion
SR-OSPF	segment routing OSPF
SR-TE	segment routing traffic engineering
SSH	secure shell
SSM	source-specific multicast synchronization status messaging
SSU	system synchronization unit
S-TAG	service VLAN tag
STM	synchronous transport module
STM1	synchronous transport module, level 1
STP	spanning tree protocol
STS	synchronous transport signal
SVC	switched virtual circuit
SVEC	synchronization vector
SYN	synchronize
TACACS+	Terminal Access Controller Access-Control System Plus
TC	traffic class (formerly known as EXP bits)
TCP	transmission control protocol
TDA	transmit diversity antenna
TDEV	time deviation
TDM	time division multiplexing
TE	traffic engineering
TEDB	traffic engineering database
TEID	tunnel endpoint identifier
TEP	tunnel endpoint
TFTP	trivial file transfer protocol
T-LDP	targeted LDP
TLS	transport layer security
TLV	type length value

Table 125 **Acronyms (Continued)**

Acronym	Expansion
TM	traffic management
ToD	time of day
ToS	type of service
T-PE	terminating provider edge router
TPID	tag protocol identifier
TPIF	IEEE C37.94 teleprotection interface
TPMR	two-port MAC relay
TPS	transmission protection switching
TSoP	Transparent SDH/SONET over Packet
TTL	time to live
TTLS	tunneled transport layer security
TTM	tunnel table manager
TU	tributary unit
TUG	tributary unit group
TWAMP	two-way active measurement protocol
U-APS	unidirectional automatic protection switching
UAS	unavailable seconds
UBR	unspecified bit rate
UDP	user datagram protocol
UFD	unidirectional forwarding detection
UMH	upstream multicast hop
UMTS	Universal Mobile Telecommunications System (3G)
UNI	user-to-network interface
uRPF	unicast reverse path forwarding
V.11	ITU-T V-series Recommendation 11
V.24	ITU-T V-series Recommendation 24
V.35	ITU-T V-series Recommendation 35

Table 125 **Acronyms (Continued)**

Acronym	Expansion
VC	virtual circuit
VCB	voice conference bridge
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCI	virtual circuit identifier
VID	VLAN ID
VLAN	virtual LAN
VLL	virtual leased line
VM	virtual machine
VoIP	voice over IP
Vp	peak voltage
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network
VRF	virtual routing and forwarding table
VRRP	virtual router redundancy protocol
VSE	vendor-specific extension
VSI	virtual switch instance
VSO	vendor-specific option
VT	virtual trunk virtual tributary
VTG	virtual tributary group
Wavence	formerly 9500 MPR (Microwave Packet Radio)
WCDMA	wideband code division multiple access (transmission protocol used in UMTS networks)

Table 125 **Acronyms (Continued)**

Acronym	Expansion
WRED	weighted random early discard
WTR	wait to restore
X.21	ITU-T X-series Recommendation 21
XOR	exclusive-OR
XRO	exclude route object

9 Standards and Protocol Support

This chapter lists the 7705 SAR compliance with EMC, environmental, and safety standards, telecom standards, and supported protocols:

Table 126 EMC Industrial Standards Compliance

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
IEEE 1613:2009 + A1:2011	IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations	✓[1]		✓[3]		✓[2]	✓[1]	✓[3]	✓[3]		
IEEE 1613.1-2013	IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Transmission and Distribution Facilities	✓[4]		✓[7]		✓[5]	✓[6]	✓[7]	✓[7]		
IEEE Std C37.90	IEEE Standard for relays and relay systems associated with Electric Power Apparatus	✓		✓		✓	✓	✓	✓		
IEEE Std C37.90.1	Surge Withstand Capability (SWC) Tests	✓		✓		✓	✓	✓	✓		
IEEE Std C37.90.2	Withstand Capability of Relay Systems to Radiated Electromagnetic Interference from Transceivers	✓		✓		✓	✓	✓	✓		
IEEE Std C37.90.3	IEEE Standard Electrostatic Discharge Tests for Protective Relays	✓		✓		✓	✓	✓	✓		
EN 50121-4	Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 62236-4	Electromagnetic Compatibility – Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 61000-6-2	Generic standards – Immunity for industrial environments	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 61000-6-4	Generic standards – Emissions standard for industrial environments	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 61000-6-5	Generic standards – immunity for equipment used in power station and substation environment	✓		✓		✓	✓	✓	✓		
IEC 61850-3	Communication networks and systems for power utility automation - Part 3: General requirements	✓		✓		✓	✓[8]	✓	✓		
IEC/AS 60870.2.1	Telecontrol equipment and systems. Operating conditions. Power supply and electromagnetic compatibility	✓		✓		✓	✓	✓	✓		

Notes:

1. Performance Class 1
2. Performance Class 1 (Class 2 with Optics interfaces only)
3. Performance Class 2
4. Zone A; Performance Class 1
5. Zone A; Performance Class 1 (Class 2 with Optics interfaces only)
6. Zone B; Performance Class 1
7. Zone A; Performance Class 2
8. With the exception of DC surges

Table 127 EMC Regulatory and Customer Standards Compliance

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
IEC 61000-4-2	Electrostatic discharge immunity test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 61000-4-3	Radiated electromagnetic field immunity test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 61000-4-4	Electrical fast transient/burst immunity test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 61000-4-5	Surge immunity test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 61000-4-6	Immunity to conducted disturbances	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 61000-4-8	Power frequency magnetic field immunity test	✓		✓		✓	✓	✓	✓		
IEC 61000-4-9	Pulse Magnetic field immunity test	✓		✓		✓	✓	✓	✓		
IEC 61000-4-10	Damped Oscillatory Magnetic Field	✓		✓		✓	✓	✓	✓		
IEC 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests	✓	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓	✓[1]	✓	✓
IEC 61000-4-12	Oscillatory wave immunity test	✓		✓		✓	✓	✓	✓		
IEC 61000-4-16	Conducted immunity 0 Hz - 150 kHz	✓		✓		✓	✓	✓	✓		
IEC 61000-4-17	Ripple on d.c. input power port immunity test	✓		✓		✓	✓	✓	✓		
IEC 61000-4-18	Damped oscillatory wave immunity test	✓		✓		✓	✓	✓	✓		
IEC 61000-4-29	Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests	✓		✓		✓	✓	✓	✓		
IEC 61000-3-2	Limits for harmonic current emissions (equipment input current <16A per phase)	✓	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓	✓[1]	✓	✓

Table 127 **EMC Regulatory and Customer Standards Compliance (Continued)**

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
IEC 61000-3-3	Limits for voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current <16A	✓	✓[1]	✓[1]	✓[1]	✓[1]	✓[1]	✓	✓[1]	✓	✓
ITU-T K.20 (DC Ports)	Resistibility of telecommunication equipment installed in a telecommunications centre to overvoltages and overcurrents	✓	✓	✓	✓	✓	✓	✓	✓		
ITU-T K.44	Resistibility tests for telecommunication equipment exposed to overvoltages and overcurrents - Basic Recommendation									✓	✓
ETSI 300 132-2	Power supply interface at the input to telecommunications and datacom (ICT) equipment; Part 2: Operated by -48 V direct current (dc)	✓	✓	✓	✓	✓	✓	✓	✓	✓	
ETSI 300 132-3	Power supply interface at the input to telecommunications equipment; Part 3: Operated by rectified current source, alternating current source or direct current source up to 400V	✓	✓[1]	✓[1]	✓[1]			✓	✓[1]	✓	✓
EN 300 386	Telecommunication network equipment; ElectroMagnetic Compatibility (EMC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ES 201 468	Electromagnetic compatibility and Radio spectrum Matters (ERM); Additional ElectroMagnetic Compatibility (EMC) requirements and resistibility requirements for telecommunications equipment for enhanced availability of service in specific applications	✓		✓	✓	✓	✓				✓
EN 55024	Information technology equipment - Immunity characteristics - Limits and methods of measurements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Telcordia GR-1089-CORE	EMC and Electrical Safety - Generic Criteria for Network Telecommunications Equipment	✓	✓	✓	✓	✓	✓	✓	✓		
AS/NZS CISPR 32	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[3]	✓[3]
FCC Part 15, Subpart B	Radio Frequency devices- Unintentional Radiators (Radiated & Conducted Emissions)	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[3]	✓[3]

Table 127 EMC Regulatory and Customer Standards Compliance (Continued)

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
ICES-003	Information Technology Equipment (ITE) — Limits and methods of measurement	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[3]	✓[3]
EN 55032	Electromagnetic compatibility of multimedia equipment – Emission requirements	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]
CISPR 32	Electromagnetic compatibility of multimedia equipment – Emission requirements	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]	✓[2]
GS7 EMC	Electromagnetic Standard Compatibility (BT standard)	✓		✓	✓	✓	✓	✓			✓
KC Notice Emission (KN32) and Immunity (KN35) (South Korea)	EMS standard: NRRA notice	✓	✓	✓	✓	✓	✓	✓	✓		

Notes:

1. With external AC/DC power supply
2. Class A
3. Class B

Table 128 Environmental Standards Compliance

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
IEEE 1613:2009 + A1:2011	Environmental and Testing Requirements for Communications Networking Devices	✓[1]		✓		✓[1]	✓[1]	✓	✓		
IEC 61850-3	Communication networks and systems for power utility automation - Part 3: General requirements	✓[2]		✓[2]		✓[2]	✓[2]	✓[2]	✓[2]		
IEC 60068-2-1	Environmental testing – Part 2-1: Tests – Test A: Cold	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 60068-2-2	Environmental testing - Part 2-2: Tests - Test B: Dry heat	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC 60068-2-30	Environmental testing - Part 2: Tests. Test Db and guidance: Damp heat, cyclic (12 + 12-hour cycle)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 128 Environmental Standards Compliance (Continued)

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
IEC 60255-21-2	Electrical relays - Part 21: Vibration, shock, bump and seismic tests on measuring relays and protection equipment - Section Two: Shock and bump tests	✓		✓		✓	✓	✓	✓		
ETSI 300 753 Class 3.2	Acoustic noise emitted by telecommunications equipment	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Telcordia GR-63-CORE	NEBS Requirements: Physical Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ETSI EN 300 019-2-1 Class 1.2	Specification of environmental tests; Storage	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ETSI EN 300 019-2-2 Class 2.3	Specification of environmental tests; Transportation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ETSI EN 300 019-2-3 Class 3.2	Specification of environmental tests; Stationary use at weatherprotected locations	✓	✓	✓	✓	✓	✓	✓	✓		
ETSI EN 300 019-2-4 Class T4.1	Specification of environmental tests; Stationary use at non-weatherprotected locations									✓	✓
Telcordia GR-3108-CORE	Generic Requirements for Network Equipment in the Outside Plant (OSP)	✓[3]	✓[3]	✓[3]	✓[3]	✓[3]		✓[3]	✓[3]	✓[4]	✓[4]
Telcordia GR-950-CORE	Generic Requirements for ONU Closures and ONU Systems									✓	✓
“GR-3108 Class 3 Section 6.2 IEC 60068-2-52 - Severity 3 MIL-STD-810G Method 509.5 EN 60721-3-3 Class 3C4 EN 60068-2-11: Salt Mist EN 50155 Class ST4”	Conformal Coating[5]	✓			✓	✓		✓	✓		

Notes:

1. Forced air system; uses fans
2. Normal environmental conditions as per IEC 61850-3 ed.2
3. Class 2
4. Class 4
5. Conformal coating is available as an orderable option

Table 129 Safety Standards Compliance

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
UL/CSA 60950-1	Information technology equipment - Safety - Part 1: General requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IEC/EN 60950-1	Information technology equipment - Safety - Part 1: General requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
UL/CSA 62368-1	Audio/video, information and communication technology equipment - Part 1: Safety requirements		✓	✓	✓	✓	✓				✓
IEC/EN 62368-1	Audio/video, information and communication technology equipment - Part 1: Safety requirements	✓	✓	✓	✓	✓	✓				✓
AS/NZS 60950-1	Information technology equipment - Safety - Part 1: General requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AS/NZS 62368-1	Audio/video, information and communication technology equipment, Part 1: Safety requirements		✓		✓	✓	✓				✓
IEC/EN 60825-1 and 2	Safety of laser products - Part 1: Equipment classification and requirements Part 2: Safety of optical fibre communication systems (OFCS)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
UL/CSA 60950-22	Information Technology Equipment - Safety - Part 22: Equipment to be Installed Outdoors									✓	✓
CSA–C22.2 No.94	Special Purpose Enclosures									✓	✓
UL50	Enclosures for Electrical Equipment, Non-Environmental Consideration									✓	✓
IEC/EN 60950-22	Information technology equipment. Equipment to be installed Outdoors.									✓	✓
IEC 60529	Degrees of Protection Provided by Enclosures (IP Code)	✓[1]	✓[2]	✓[2]	✓[1]	✓[1]	✓[1]	✓[2]	✓[2]	✓[3]	✓[3]

Notes:

1. IP20
2. IP40
3. IP65

Table 130 Telecom Interface Compliance

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
IC CS-03 Issue 9	Compliance Specification for Terminal Equipment, Terminal Systems, Network Protection Devices, Connection Arrangements and Hearing Aids Compatibility	✓	✓		✓	✓	✓	✓			
ACTA TIA-968-B	Telecommunications - Telephone Terminal Equipment - Technical Requirements for Connection of Terminal Equipment to the Telephone Network	✓	✓		✓	✓	✓	✓			
AS/ACIF S016 (Australia)	Requirements for Customer Equipment for connection to hierarchical digital interfaces	✓	✓		✓	✓	✓	✓			
ATIS-06000403	Network and Customer Installation Interfaces- DS1 Electrical Interfaces	✓	✓		✓	✓	✓	✓			
ANSI/TIA/EIA-422-B (RS422)	Electrical Characteristics for balanced voltage digital interfaces circuits					✓	✓				
ITU-T G.825	The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)					✓	✓				
ITU-T G.703	Physical/electrical characteristics of hierarchical digital interfaces	✓	✓		✓	✓	✓	✓			
ITU-T G.712 (E&M)	Transmission performance characteristics of pulse code modulation channels					✓	✓				
ITU-T G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy					✓	✓				
ITU-T V.24 (RS232)	List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)					✓	✓	✓	✓		
ITU-T V.28 (V35)	Electrical characteristics for unbalanced double-current interchange circuits					✓	✓				
ITU-T V.36 (V35)	Modems for synchronous data transmission using 60-108 kHz group band circuits					✓	✓				

Table 130 Telecom Interface Compliance (Continued)

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
ITU-T V.11 / X.27 (RS-422)	Electrical characteristics for balanced double current interchange circuits operating at data signalling rates up to 10 Mbit/s					✓	✓				
ITU-T X.21 (RS-422)	Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks					✓	✓				
IEEE 802.3at (POE)	Data Terminal Equipment Power via the Media Dependent Interfaces Enhancements				✓			✓	✓	✓	✓

Table 131 Directives, Regional Approvals and Certifications Compliance

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
EU Directive 2014/30/EU (EMC)	Electromagnetic Compatibility (EMC)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
EU Directive 2014/35/EU (LVD)	Low Voltage Directive (LVD)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
EU Directive 2012/19/EU (WEEE)	Waste Electrical and Electronic Equipment (WEEE)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
EU Directive 2011/65/EU (RoHS)	EU Directive 2011/65/EU Restriction of the use of certain Hazardous Substances in Electrical and Electronic Equipment (Recast) Directive (including Commission Delegated Directive (EU) 2015/863)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
CE Mark		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
UKCA Mark		✓	✓	✓	✓	✓	✓	✓	✓		✓
CRoHS Logo; Ministry of Information Industry order No.39		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
China (MII NAL) Network Access License			✓		✓	✓	✓	✓		✓	

Table 131 **Directives, Regional Approvals and Certifications Compliance (Continued)**

Standard	Title	Platform									
		SAR-X	SAR-A	SAR-Ax	SAR-M	SAR-8	SAR-18	SAR-H	SAR-Hc	SAR-W	SAR-Wx
South Korea (KC Mark)		✓	✓	✓	✓	✓	✓	✓	✓		
Australia (RCM Mark)		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Japan (VCCI Mark)		✓	✓	✓	✓	✓	✓	✓			
NEBS Level 3		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TL9000 certified		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ISO 14001 certified		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ISO 9001 certified		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Security Standards

FIPS 140-2—Federal Information Processing Standard publication 140-2, Security Requirements for Cryptographic Modules

Telecom Standards

ANSI/TIA/EIA-232-C—Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange

IEEE 802.1ad—IEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks

IEEE 802.1ag—Service Layer OAM

IEEE 802.1p/q—VLAN Tagging

IEEE 802.3—10BaseT

IEEE 802.3ab—1000BaseT

IEEE 802.3ah—Ethernet OAM

IEEE 802.3u—100BaseTX

IEEE 802.3x —Flow Control

IEEE 802.3z—1000BaseSX/LX

IEEE 802.3-2008—Revised base standard

IEEE 802.1AX-2008—Link Aggregation Task Force (transferred from IEEE 802.3ad)

IEEE C37.94-2017—N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment

ITU-T G.704—Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

ITU-T G.707—Network node interface for the Synchronous Digital Hierarchy (SDH)

ITU-T G.826—End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

ITU-T G.8032 — Ethernet Ring Protection Switching

ITU-T G.984.1—Gigabit-capable passive optical networks (GPON): general characteristics

ITU-T Y.1564—Ethernet service activation test methodology

ITU-T Y.1731—OAM functions and mechanisms for Ethernet-based networks

Protocol Support

ATM

AF-PHY-0086.001—Inverse Multiplexing for ATM (IMA)

af-tm-0121.000—Traffic Management Specification Version 4.1, March 1999

GR-1113-CORE—Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994

GR-1248-CORE—Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996

ITU-T Recommendation I.432.1—B-ISDN user-network interface - Physical layer specification: General characteristics

ITU-T Recommendation I.610—B-ISDN Operation and Maintenance Principles and Functions version 11/95

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

BFD

draft-ietf-bfd-mib-00.txt—Bidirectional Forwarding Detection Management Information Base

draft-ietf-bfd-base-o5.txt—Bidirectional Forwarding Detection

draft-ietf-bfd-v4v6-1hop-06.txt—BFD IPv4 and IPv6 (Single Hop)

draft-ietf-bfd-multihop-06.txt—BFD for Multi-hop Paths

BGP

RFC 1397—BGP Default Route Advertisement

RFC 1997—BGP Communities Attribute

RFC 2385—Protection of BGP Sessions via the TCP MD5 Signature Option

RFC 2439—BGP Route Flap Dampening

RFC 2545—Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing

RFC 2918—Route Refresh Capability for BGP-4

RFC 3107—Carrying Label Information in BGP-4

RFC 3392—Capabilities Advertisement with BGP-4

RFC 4271—BGP-4 (previously RFC 1771)

RFC 4360—BGP Extended Communities Attribute

RFC 4364—BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2574bis BGP/MPLS VPNs)

RFC 4456—BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)

RFC 4486—Subcodes for BGP Cease Notification Message

RFC 4684—Constrained Route Distribution for Border Gateway Protocol/ MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)

RFC 4724—Graceful Restart Mechanism for BGP - GR Helper

RFC 4760—Multi-protocol Extensions for BGP (previously RFC 2858)

RFC 4893—BGP Support for Four-octet AS Number Space

RFC 6513—Multicast in MPLS/BGP IP VPNs

RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs

draft-ietf-idr-add-paths-04.txt—Advertisement of Multiple Paths in BGP

draft-ietf-idr-add-paths-guidelines-00.txt—Best Practices for Advertisement of Multiple Paths in BGP

DHCP/DHCPv6

RFC 1534—Interoperation between DHCP and BOOTP

RFC 2131—Dynamic Host Configuration Protocol (REV)

RFC 2132—DHCP Options and BOOTP Vendor Extensions

RFC 3046—DHCP Relay Agent Information Option (Option 82)

RFC 3315—Dynamic Host Configuration Protocol for IPv6

RFC 3736—Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

Differentiated Services

RFC 2474—Definition of the DS Field in the IPv4 and IPv6 Headers

RFC 2597—Assured Forwarding PHB Group

RFC 2598—An Expedited Forwarding PHB

RFC 3140—Per-Hop Behavior Identification Codes

Digital Data Network Management

V.35

RS-232 (also known as EIA/TIA-232)

X.21

ECMP

RFC 2992—Analysis of an Equal-Cost Multi-Path Algorithm

Ethernet VPN (EVPN)

RFC 7432—BGP MPLS-Based Ethernet VPN

draft-ietf-bess-evpn-vpls-seamless-integ—(PBB-)EVPN Seamless Integration with (PBB-)VPLS

draft-ietf-bess-evpn-vpws—Virtual Private Wire Service support in Ethernet VPN

Frame Relay

ANSI T1.617 Annex D—Signalling Specification For Frame Relay Bearer Service

ITU-T Q.922 Annex A—Digital Subscriber Signalling System No. 1 (DSS1) data link layer - ISDN data link layer specification for frame mode bearer services

FRF.1.2—PVC User-to-Network Interface (UNI) Implementation Agreement

FRF.12—Frame Relay Fragmentation Implementation Agreement

RFC 2427—Multiprotocol Interconnect over Frame Relay

GRE

RFC 2784—Generic Routing Encapsulation (GRE)

Internet Protocol (IP) – Version 4

RFC 768—User Datagram Protocol

RFC 791—Internet Protocol

RFC 792—Internet Control Message Protocol

RFC 793—Transmission Control Protocol

RFC 826—Ethernet Address Resolution Protocol

RFC 854—Telnet Protocol Specification

RFC 1350—The TFTP Protocol (Rev. 2)

RFC 1812—Requirements for IPv4 Routers

RFC 3021—Using 31-Bit Prefixes on IPv4 Point-to-Point Links

Internet Protocol (IP) – Version 6

RFC 2460—Internet Protocol, Version 6 (IPv6) Specification

RFC 2462—IPv6 Stateless Address Autoconfiguration

RFC 2464—Transmission of IPv6 Packets over Ethernet Networks

RFC 3587—IPv6 Global Unicast Address Format

RFC 3595—Textual Conventions for IPv6 Flow Label

RFC 4007—IPv6 Scoped Address Architecture

RFC 4193—Unique Local IPv6 Unicast Addresses

RFC 4291—IPv6 Addressing Architecture

RFC 4443—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification

RFC 4649—DHCPv6 Relay Agent Remote-ID Option

RFC 4861—Neighbor Discovery for IP version 6 (IPv6)

RFC 5095—Deprecation of Type 0 Routing Headers in IPv6

RFC 5952—A Recommendation for IPv6 Address Text Representation

IPSec

ITU-T X.690 (2002)—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

PKCS #12 Personal Information Exchange Syntax Standard

RFC 2315—PKCS #7: Cryptographic Message Syntax

RFC 2409—The Internet Key Exchange (IKE)

RFC 2986—PKCS #10: Certification Request Syntax Specification

RFC 3706—A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

RFC 3947—Negotiation of NAT-Traversal in the IKE

RFC 3948—UDP Encapsulation of IPsec ESP Packets

RFC 4301—Security Architecture for the Internet Protocol

RFC 4303—IP Encapsulating Security Payload (ESP)

RFC 4210—Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)

RFC 4211—Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)

RFC 4945—The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

RFC 5280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

RFC 5996—Internet Key Exchange Protocol Version 2 (IKEv2)

RFC 7383—Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation

IS-IS

RFC 1142—OSI IS-IS Intra-domain Routing Protocol (ISO 10589)

RFC 1195—Use of OSI IS-IS for routing in TCP/IP & dual environments

RFC 2763—Dynamic Hostname Exchange for IS-IS

RFC 2966—Domain-wide Prefix Distribution with Two-Level IS-IS

RFC 2973—IS-IS Mesh Groups

RFC 3373—Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies

RFC 3567—Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication

RFC 3719—Recommendations for Interoperable Networks using IS-IS

RFC 3784—Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)

RFC 3787—Recommendations for Interoperable IP Networks

RFC 4205 for Shared Risk Link Group (SRLG) TLV

RFC 4971—Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information

RFC 5304—IS-IS Cryptographic Authentication

RFC 5305—IS-IS Extensions for Traffic Engineering

RFC 5308—Routing IPv6 with IS-IS

RFC 5309—Point-to-Point Operation over LAN in Link State Routing Protocols

RFC 5310—IS-IS Generic Cryptographic Authentication

RFC 6232—Purge Originator Identification TLV for IS-IS

LDP

RFC 5036—LDP Specification

RFC 5283—LDP Extension for Inter-Area Label Switched Paths

RFC 5350—-IANA Considerations for the IPv4 and IPv6 Router Alert Options

RFC 5443—LDP IGP Synchronization

RFC 5561—LDP Capabilities

RFC 6388—Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths

RFC 6512—Using Multipoint LDP When the Backbone Has No Route to the Root

RFC 6829—Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6

RFC 7552—Updates to LDP for IPv6

draft-ietf-mpls-ldp-ip-pw-capability—Controlling State Advertisements Of Non-negotiated LDP Applications

draft-ietf-mpls-oam-ipv6-rao—IPv6 Router Alert Option for MPLS OAM

draft-pdutta-mpls-ldp-adj-capability-00—LDP Adjacency Capabilities

draft-pdutta-mpls-ldp-v2-00—LDP Version 2

draft-pdutta-mpls-mldp-up-redundancy-00.txt—Upstream LSR Redundancy for Multi-point LDP Tunnels

LDP and IP FRR

RFC 5286—Basic Specification for IP Fast Reroute: Loop-Free Alternates

RFC 7490—Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)

MPLS

RFC 3031—MPLS Architecture

RFC 3032—MPLS Label Stack Encoding

RFC 3815—Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)

RFC 6790—The Use of Entropy Labels in MPLS Forwarding

MPLS – OAM

RFC 4379—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

RFC 6424— Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels

Multicast

RFC 3956—Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

RFC 3973—Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)

RFC 4610—Anycast-RP Using Protocol Independent Multicast (PIM), which is similar to RFC 3446—Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

RFC 6514—BGP Encodings and Procedures for Multicast in MPLS/IP VPNs

cisco-ipmulticast/pim-autorp-spec—Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast, which is similar to RFC 5059—Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

draft-ietf-l2vpn-vpls-pim-snooping-07—Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)

draft-ietf-mboned-msdp-deploy-nn.txt—Multicast Source Discovery Protocol (MSDP) Deployment Scenarios

Network Management

IANA-IFType-MIB

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

RFC 1157—SNMPv1

RFC 1850—OSPF-MIB

RFC 1907—SNMPv2-MIB

RFC 2011—IP-MIB

RFC 2012—TCP-MIB

RFC 2013—UDP-MIB

RFC 2030—Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

RFC 2096—IP-FORWARD-MIB

RFC 2138—RADIUS

RFC 2206—RSVP-MIB

RFC 2571—SNMP-FRAMEWORKMIB

RFC 2572—SNMP-MPD-MIB
RFC 2573—SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574—SNMP-USER-BASED-SMMIB
RFC 2575—SNMP-VIEW-BASED ACM-MIB
RFC 2576—SNMP-COMMUNITY-MIB
RFC 2588—SONET-MIB
RFC 2665—EtherLike-MIB
RFC 2819—RMON-MIB
RFC 2863—IF-MIB
RFC 2864—INVERTED-STACK-MIB
RFC 3014—NOTIFICATION-LOG MIB
RFC 3164—The BSD Syslog Protocol
RFC 3273—HCRMON-MIB
RFC 3411—An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412—Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413—Simple Network Management Protocol (SNMP) Applications
RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418—SNMP MIB
RFC 3954—Cisco Systems NetFlow Services Export Version 9
RFC 5101—Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information
RFC 5102—Information Model for IP Flow Information Export
draft-ietf-disman-alarm-mib-04.txt
draft-ietf-mpls-ldp-mib-07.txt
draft-ietf-ospf-mib-update-04.txt
draft-ietf-mpls-lsr-mib-06.txt
draft-ietf-mpls-te-mib-04.txt
TMF 509/613—Network Connectivity Model

OSPF

RFC 1765—OSPF Database Overflow
RFC 2328—OSPF Version 2
RFC 2370—Opaque LSA Support
RFC 2740—OSPF for IPv6
RFC 3101—OSPF NSSA Option

RFC 3137—OSPF Stub Router Advertisement

RFC 3509—Alternative Implementations of OSPF Area Border Routers

RFC 3623—Graceful OSPF Restart (support for Helper mode)

RFC 3630—Traffic Engineering (TE) Extensions to OSPF

RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV

RFC 4577—OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) (support for basic OSPF at PE-CE links)

RFC 4915—Multi-Topology (MT) Routing in OSPF

RFC 4970—Extensions to OSPF for Advertising Optional Router Capabilities

RFC 5185—OSPF Multi-Area Adjacency

OSPFv3

RFC 4552—Authentication/Confidentiality for OSPFv3

PPP

RFC 1332—PPP Internet Protocol Control Protocol (IPCP)

RFC 1570—PPP LCP Extensions

RFC 1619—PPP over SONET/SDH

RFC 1661—The Point-to-Point Protocol (PPP)

RFC 1662—PPP in HDLC-like Framing

RFC 1989—PPP Link Quality Monitoring

RFC 1990—The PPP Multilink Protocol (MP)

RFC 2686—The Multi-Class Extension to Multi-Link PPP

Pseudowires

Metro Ethernet Forum—Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks

RFC 3550—RTP: A Transport Protocol for Real-Time Applications

RFC 3985—Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture

RFC 4385—Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN

RFC 4446—IANA Allocation for PWE3

RFC 4447—Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)

RFC 4448—Encapsulation Methods for Transport of Ethernet over MPLS Networks

RFC 4553—Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)

RFC 4717—Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks

RFC 4618—Encapsulation Methods for Transport of PPP/High-Level Data Link Control (HDLC) over MPLS Networks

RFC 4619—Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks

RFC 4816—Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service

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

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

draft-ietf-pwe3-redundancy-02.txt—Pseudowire (PW) Redundancy

RIP

RFC 1058—Routing Information Protocol

RFC 2453—RIP Version 2

RADIUS

RFC 2865—Remote Authentication Dial In User Service

RFC 2866—RADIUS Accounting

RSVP-TE and FRR

RFC 2430—A Provider Architecture for DiffServ & TE

RFC 2702—Requirements for Traffic Engineering over MPLS

RFC 2747—RSVP Cryptographic Authentication

RFC 2961—RSVP Refresh Overhead Reduction Extensions

RFC 3097—RSVP Cryptographic Authentication - Updated Message Type Value

RFC 3209—Extensions to RSVP for LSP Tunnels

RFC 3210—Applicability Statement for Extensions to RSVP for LSP Tunnels

RFC 3477—Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)

RFC 4090—Fast Reroute Extensions to RSVP-TE for LSP Tunnels

RFC 5440—Path Computation Element (PCE) Communication Protocol (PCEP)

draft-ietf-pce-stateful-pce—PCEP Extensions for Stateful PCE

draft-ietf-pce-segment-routing—PCEP Extensions for Segment Routing

draft-alvarez-pce-path-profiles—PCE Path Profiles

Segment Routing (SR)

draft-francois-rtgwg-segment-routing-ti-lfa-04—Topology Independent Fast Reroute using Segment Routing

draft-gredler-idr-bgp-ls-segment-routing-ext-03—BGP Link-State extensions for Segment Routing

draft-ietf-isis-segment-routing-extensions-04—IS-IS Extensions for Segment Routing

draft-ietf-mpls-spring-lsp-ping-02—Label Switched Path (LSP) Ping/Trace for Segment Routing Networks Using MPLS Dataplane

draft-ietf-ospf-segment-routing-extensions-04—OSPF Extensions for Segment Routing

SONET/SDH

GR-253-CORE—SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000

ITU-T Recommendation G.841—Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

SSH

RFC 4253—The Secure Shell (SSH) Transport Layer Protocol

draft-ietf-secsh-architecture.txt—SSH Protocol Architecture

draft-ietf-secsh-userauth.txt—SSH Authentication Protocol

draft-ietf-secsh-connection.txt—SSH Connection Protocol

draft-ietf-secsh- newmodes.txt—SSH Transport Layer Encryption Modes

draft-ietf-secsh-filexfer-13.txt—SSH File Transfer Protocol

Synchronization

G.781—Synchronization layer functions, 2001/09/17

G.803—Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813—Timing characteristics of SDH equipment slave clocks (SEC)

G.823—The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy, 2003/03/16

G.824—The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy, 2003/03/16

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

IEC/IEEE 61850-9-3—Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation

IEEE C37.238-2017 - IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications

IEEE Std 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

IEEE Std 1588-2008—IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, Annex E – Transport of PTP over User Datagram Protocol over Internet Protocol Version 6

ITU-T G.8264—Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008

ITU-T G.8265.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for frequency synchronization, issued 10/2010

ITU-T G.8275.1—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014

ITU-T G.8275.2—Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for time/phase synchronization with partial timing support from the network, issued 06/2016

RFC 5905—Network Time Protocol Version 4: Protocol and Algorithms Specification

TACACS+

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

TWAMP

RFC 5357—A Two-Way Active Measurement Protocol (TWAMP)

VPLS

RFC 4762—Virtual Private LAN Services Using LDP

VRRP

RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol

RFC 3768 Virtual Router Redundancy Protocol

RFC 5798 Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

Proprietary MIBs

TIMETRA-ATM-MIB.mib
TIMETRA-CAPABILITY-7705-V1.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-SAP-MIB.mib
TIMETRA-SDP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRRP-MIB.mib

Customer Document and Product Support

Customer Documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation Feedback

Customer Documentation Feedback

3HE 17553 AAAB TQZZA