7210 SAS M, X OS
Router Configuration Guide

Software Version: 7210 SAS OS 5.0 Rev. 05
April 2013
Document Part Number: 93-0426-01-05

TABLE OF CONTENTS

Filter Policies

List of Tables

List of Figures

Preface

About This Guide

This guide describes logical IP routing interfaces, IP and MAC-based filtering support provided by the 7210 SAS M, X and presents configuration and implementation examples.

All the variants of 7210 SAS-M can be configured in two modes, that is in network mode and in access-uplink mode. In network mode configuration 7210 SAS-M uses IP/MPLS to provide service transport. In access-uplink mode configuration 7210 SAS-M uses Ethernet QinQ technology to provide service transport. The mode can be selected by configuring the BOF appropriately.

Note: In either mode, it is expected that the user will only configure the required CLI parameters appropriate for the mode he intends to use. Unless otherwise noted, most of the configuration is similar in both the Network mode and Access uplink mode.

Note :Only 7210 SAS-M supports access-uplink mode. 7210 SAS-X does not support access-uplink mode.

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

Audience

This manual is intended for network administrators who are responsible for configuring the 7210 SAS-Series routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols, standards, and services described in this manual include the following:

- IP router configuration
- IP and MAC-based filters

List of Technical Publications

The 7210-SAS M, X OS documentation set is composed of the following books:

- 7210-SAS M, X OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.
- 7210-SAS M, X OS System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.
- 7210-SAS M, X OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.
- 7210-SAS M, X OS OS Router Configuration Guide

  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP and MAC-based filtering.
- 7210-SAS M, X OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for BGP, OSPF, IS-IS, and route policies.
- 7210-SAS M, X OS MPLS Guide

  This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).
- 7210 SAS M Services Guide

  This guide describes how to configure service parameters such as customer information and user services.
- 7210-SAS M, X OS OAM and Diagnostic Guide

  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.
- 7210 SAS M Quality of Service Guide

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

Technical Support

If you purchased a service agreement for your 7210 SAS router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center at:

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

Getting Started

In This Chapter

This chapter provides process flow information to configure routing entities, virtual routers, IP and MAC filters.

Alcatel-Lucent 7210 SAS-Series Router Configuration Process

Table 1 lists the tasks necessary to configure logical IP routing interfaces, virtual routers, IP and MAC-based filtering.

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

Table 1: Configuration Process

Area	Task	Chapter
Router configuration	Configure router parameters, including router interfaces, addresses, router IDs, and autonomous systems.	IP Router Configuration on page 17
	IP and MAC filters	Filter Policies on page 213
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 309

IP Router Configuration

In This Chapter

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

Topics in this chapter include:

Configuring IP Router Parameters

In order to provision services on a 7210 SAS router, logical IP routing interfaces must be configured to associate attributes such as an IP address or the system with the IP interface.

A special type of IP interface is the system interface. A system interface must have an IP address with a 32-bit subnet mask. The system interface is used as the router identifier by higher-level protocols such as OSPF and BGP, unless overwritten by an explicit router ID.

The following router features can be configured:

- Interfaces on page 18
- Autonomous Systems (AS) on page 22

Interfaces

7210 SAS routers use different types of interfaces for various functions. Interfaces must be configured with parameters such as the interface type (system) and address. A port is not associated with a system interface. An interface can be associated with the system (loopback address).

Network Interface

A network interface (a logical IP routing interface) can be configured on a physical port.

System Interface

The system interface is associated with the network entity (such as a specific router or switch), not a specific interface. The system interface is also referred to as the loopback address. The system interface is associated during the configuration of the following entities:

- The termination point of service tunnels
- The hops when configuring MPLS paths and LSPs
- The addresses on a target router for BGP and LDP peering

The system interface is used to preserve connectivity (when routing reconvergence is possible) when an interface fails or is removed. The system interface is also referred to as the loopback address and is used as the router identifier. A system interface must have an IP address with a 32-bit subnet mask.

Router ID

The router ID, a 32-bit number, uniquely identifies the router within an autonomous system (AS). In protocols such as OSPF, routing information is exchanged between areas, groups of networks that share routing information. It can be set to be the same as the loopback address. The router ID is used by both OSPF and BGP routing protocols in the routing table manager instance.

There are several ways to obtain the router ID. On each 7210 SAS M, X router, the router ID can be derived in the following ways.

- Define the value in the **config>router** *router-id* context. The value becomes the router ID.
- Configure the system interface with an IP address in the **config>router>interface** *ip-int-name* context. If the router ID is not manually configured in the **config>router** *router-id* context, then the system interface acts as the router ID.
- If neither the system interface or router ID are implicitly specified, then the router ID is inherited from the last four bytes of the MAC address.
- The router can be derived on the protocol level.

Autonomous Systems (AS)

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

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

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

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

Proxy ARP

Proxy ARP is the technique in which a router answers ARP requests intended for another node. The router appears to be present on the same network as the “real” node that is the target of the ARP and takes responsibility for routing packets to the “real” destination. Proxy ARP can help nodes on a subnet reach remote subnets without configuring routing or a default gateway. Typical routers only support proxy ARP for directly attached networks; the router is targeted to support proxy ARP for all known networks in the routing instance where the virtual interface proxy ARP is configured.

In order to support DSLAM 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 and prefix lists that determine for which source hosts proxy ARP will be attempted.

In addition, the proxy ARP implementation will support the ability to respond for other hosts within the local subnet domain. This is needed in environments such as DSL where multiple hosts are in the same subnet but can not reach each other directly.

Static ARP is used when an Alcatel-Lucent router needs to know about a device on an interface that cannot or does not respond to ARP requests. Thus, the configuration can state that if it has a packet with a certain IP address to send it to the corresponding ARP address. Use proxy ARP so the router responds to ARP requests on behalf of another device.

Internet Protocol Versions

The TiMOS implements IP routing functionality, providing support for IP version 4 (IPv4) and IP version 6 (IPv6). IP version 6 (RFC 1883, Internet Protocol, Version 6 (IPv6)) is a newer version of the Internet Protocol designed as a successor to IP version 4 (IPv4) (RFC-791, Internet Protocol). The changes from IPv4 to IPv6 effects the following categories:

- 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 simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a scope field to multicast addresses. Also, a new type of address called an anycast address is defined that is used to send a packet to any one of a group of nodes.
- Header format simplification — Some IPv4 header fields have been dropped or made optional to reduce the common-case 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 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.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Prio. |                   Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: IPv6 Header Format

Table 2: IPv6 Header Field Descriptions

Field	Description
Version	4-bit Internet Protocol version number = 6.
Prio.	4-bit priority value.
Flow Label	24-bit flow label.
Payload Length	6-bit unsigned integer. The length of payload, for example, the rest of the packet following the IPv6 header, in octets. If the value is zero, the payload length iscarried in a jumbo payload hop-by-hop option.
Next Header	8-bit selector. Identifies the type of header immediately following the IPv6 header. This field uses the same values as the IPv4 protocol field.
Hop Limit	8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if the hop limit is decremented to zero.
Source Addres	128-bit address of the originator of the packet.
Destination Address	128-bit address of the intended recipient of the packet (possibly not the ultimate recipient if a routing header is present).

IPv6 Applications

The IPv6 applications for 7210 SAS-M and SAS-X are:

- IPv6 inband management of the node using network port IPv6 IP interface
- IPv6 transit traffic (using network port IPv6 IP interfaces)

DNS

The DNS client is extended to use IPv6 as transport and to handle the IPv6 address in the DNS AAAA resource record from an IPv4 or IPv6 DNS server. An assigned name can be used instead of an IPv6 address as IPv6 addresses are more difficult to remember than IPv4 addresses.

Bi-directional Forwarding Detection

Bi-directional Forwarding Detection (BFD) is a light-weight, low-overhead, short-duration mechanism to detect failures in the path between two systems. If a system stops receiving BFD messages for a long enough period (based on configuration) it is assumed that a failure along the path has occurred and the associated protocol or service is notified of the failure.

Listed below are the advantages of implementing the BFD mechanism:

- Used for Liveness detection over any media type
- Can be used at any protocol layer
- Proliferation of different methods and be avoided.
- Can be used with a wide range of detection times and overhead

BFD is implemented in asynchronous mode, in this mode periodic BFD control messages are used to test the path between the systems.

A path is declared operational when two-way communication has been established between both the systems. A separate BFD session is created for each communication path and data protocol between two systems.

BFD also supports the Echo function defined in draft-ietfbfd-base-04.txt, Bidirectional Forwarding Detection. In this scenario one of the systems send a sequence of BFD echo packets to the other system which loops back the echo packets within the systems forwarding plane. If many of the echo packets are lost, the BFD session is declared as down.

BFD Control Packet

The base BFD specification does not specify the encapsulation type to be used for sending BFD control packets. Choice of the appropriate encapsulation-type to be implemented is based on the network and medium. The encapsulation for BFD over IPv4 networks is specified in draft-ietf-bfd-v4v6-1hop-04.txt, *BFD for IPv4 (Single Hop)*. This specification requires that BFD control packets be sent over UDP with a destination port number of 3784 and the source port number must be within the range 49152 to 65535.

Note:

- The TTL of all transmitted BFD packets must have an IP TTL of 255
- If authentication is not enabled, all BFD packets received must have an IP TTL of 255.
- If authentication is enabled, the IP TTL should be 255. In case the IP TTL is not 255 the BFD packets are still processed, if packet passes the enabled authentication mechanism.

- If multiple BFD sessions exist between two nodes, the BFD discriminator is used to de-multiplex the BFD control packet to the appropriate BFD session.

Control Packet Format

The BFD control packet has 2 sections, a mandatory section and an optional authentication section.

```
0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Vers |  Diag   |Sta|P|F|C|A|D|R|  Detect Mult  |    Length     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       My Discriminator                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      Your Discriminator                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Desired Min TX Interval                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                   Required Min RX Interval                    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                 Required Min Echo RX Interval                 |
```

Figure 2: Mandatory Frame Format

Table 3: BFD Control Packet Field Descriptions

Field	Description
Vers	The version number of the protocol. The initial protocol version is 0.
Diag	A diagnostic code specifying the local system’s reason for the last transition of the session from Up to some other state. Possible values are: 0-No diagnostic 1-Control detection time expired 2-Echo function failed 3-Neighbor signaled session down 4-Forwarding plane reset 5-Path down 6-Concatenated path down 7-Administratively down
H Bit	The “I Hear You” bit. This bit is set to 0 if the transmitting system either is not receiving BFD packets from the remote system, or is in the process of tearing down the BFD session for some reason. Otherwise, during normal operation, it is set to 1.
D Bit	The “demand mode” bit. (Not supported)

Table 3: BFD Control Packet Field Descriptions (Continued)

Field	Description
P Bit	The poll bit. If set, the transmitting system is requesting verification of connectivity, or of a parameter change.
F Bit	The final bit. If set, the transmitting system is responding to a received BFD control packet that had the poll (P) bit set.
Rsvd	Reserved bits. These bits must be zero on transmit and ignored on receipt.
Detect Mult	The “Detect time multiplier”. In the Asynchronous mode, Detection time = Detect time Multiplier * transmit interval. If a BFD control packet is not received from the remote system within the detection time, implies that a failure has occurred.
Length	Length of the BFD control packet, in bytes.
My Discriminator	A unique, nonzero discriminator value generated by the transmitting system, used to demultiplex multiple BFD sessions between the same pair of systems.
Your Discriminator	The discriminator received from the corresponding remote system. This field reflects back the received value of my discriminator, or is zero if that value is unknown.
Desired Min TX Interval	This is the minimum interval, in microseconds, that the local system would like to use when transmitting BFD control packets.
Required Min RX Interval	This is the minimum interval, in microseconds, between received BFD control packets that this system is capable of supporting.
Required Min Echo RX Interval	This is the minimum interval, in microseconds, between received BFD echo packets that this system is capable of supporting. If this value is zero, the transmitting system does not support the receipt of BFD echo packets.

Echo Support

In the BFD echo support scenario, the 7210 SAS loops back received BFD echo messages to the original sender based on the destination IP address in the packet.

The echo function is useful when the local router does not have sufficient CPU power to handle a periodic polling rate at a high frequency. As a result, it relies on the echo sender to send a high rate of BFD echo messages through the receiver node, which is only processed by the receiver’s forwarding path. This allows the echo sender to send BFD echo packets at any rate.

The 7210 SAS supports only response to echo requests and does not support sending of echo requests.

Process Overview

The following items are components to configure basic router parameters.

- Interface — A logical IP routing interface. Once created, attributes like an IP address, port, link aggregation group or the system can be associated with the IP interface.
- Address — The address associates the device’s system name with the IP system address. An IP address must be assigned to each IP interface.
- System interface — This creates an association between the logical IP interface and the system (loopback) address. The system interface address is the circuitless address (loopback) and is used by default as the router ID for protocols such as OSPF and BGP.
- Router ID — (Optional) The router ID specifies the router's IP address.
- Autonomous system — (Optional) An autonomous system (AS) is a collection of networks that are subdivided into smaller, more manageable areas.

Configuration Notes

The following information describes router configuration guidelines.

- A system interface and associated IP address should be specified.
- Boot options file (BOF) parameters must be configured prior to configuring router parameters.
- IPv6 addressing and routing is supported only for network port IP interfaces. IPv6 based services (that is, IES and VPRN IPv6 services) are not supported in 7210.
- IPv4 and IPv6 route table lookup entries are shared. Before adding routes for IPv6 destinations, route entries in the routed lookup table needs to be allocated for IPv6 addresses. This can be done using the CLI command *config> system> resource-profile> max-ipv6-routes*. This command allocates route entries for /64 IPv6 prefix route lookups. The system does not allocate any IPv6 route entries by default and user needs to allocate some resources before using IPv6. For the command to take effect the node must be rebooted after making the change. Please see the example below and the Systems Basic guide for more information.
- A separate route table is used for IPv6 /128-bit prefix route lookup. A limited amount of IPv6 /128 prefixes route lookup entries is supported. The software enables lookups in this table by default (in other words no user configuration is required to enable IPv6 /128-bit route lookup).
- IPv6 interfaces are allowed to be created without allocating IPv6 route entries. With this only IPv6 hosts on the same subnet will be reachable.
- In 7210 SAS, the FIB is shared among all routing instances (that is, Base instance, management instance, and VPRN service instances).
- Software shutsdown control protocols (For example: OSPF) if the routing FIB (that is, either IPv4 FIB or IPv6 FIB) size limit is exceeded. Users must ensure through proper network design that the FIB size is not exceeded. Users must the available tools (that is, route policies) to ensure that all the features that share the IPv4/IPv6 FIB, do not install routes more than the available FIB size.

Configuring an IP Router with CLI

This section provides information to configure an IP router.

Topics in this section include:

Router Configuration Overview

In a 7210 SAS, an interface is a logical named entity. An interface is created by specifying an interface name under the `configure>router` context. This is the global router configuration context where objects like static routes are defined. An IP interface name can be up to 32 alphanumeric characters long, must start with a letter, and is case-sensitive; for example, the interface name "1.1.1.1" is not allowed, but "int-1.1.1.1" is allowed.

To create an interface on an Alcatel-Lucent 7210 SAS router, 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.
- Associate the interface with a system or a loopback interface.
- Configure appropriate routing protocols.

A system interface and network interface should be configured.

System Interface

The system interface is associated with the network entity (such as a specific 7210 SAS M, X), not a specific interface. The system interface is also referred to as the loopback address. The system interface is associated during the configuration of the following entities:

- The termination point of service tunnels
- The hops when configuring MPLS paths and LSPs
- The addresses on a target router for BGP and LDP peering.

The system interface is used to preserve connectivity (when routing reconvergence is possible) when an interface fails or is removed. The system interface is used as the router identifier. A system interface must have an IP address with a 32-bit subnet mask.

Network Interface

A network interface can be configured on a physical port or LAG:

- A physical or logical port

Basic Configuration

Note: Refer to each specific chapter for specific routing protocol information and command syntax to configure protocols such as OSPF and BGP.

The most basic router configuration must have the following:

- System name
- System address

The following example displays a router configuration:

```
A:ALA-A> config# info
. . .
#------------------------------------------
# Router Configuration
#------------------------------------------
    router
        interface "system"
            address 10.10.10.103/32
        exit
        interface "to-104"
            address 10.0.0.103/24
            port 1/1/1
            exit
        exit
        autonomous-system 12345
   router-id 10.10.10.103
...
     exit
     isis
     exit
...
#------------------------------------------
A:ALA-A> config#
```

Common Configuration Tasks

The following sections describe basic system tasks.

- Configuring a System Name on page 36
- Configuring Interfaces on page 37
  → Configuring a System Interface on page 37
  → Configuring a Network Interface on page 37

Configuring a System Name

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

If special characters are included in the system name string, such as spaces, #, or ?, the entire string must be enclosed in double quotes. Use the following CLI syntax to configure the system name:

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

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

The following example displays the system name output.

```
A:ALA-A>config>system# info
#------------------------------------------
# System Configuration
#------------------------------------------
        name "ALA-A"
        location "Mt.View, CA, NE corner of FERG 1 Building"
        coordinates "37.390, -122.05500 degrees lat."
        snmp
        exit
        . . .
        exit
----------------------------------------------
```

Configuring Interfaces

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

Note that the system interface cannot be deleted.

Configuring a System Interface

To configure a system interface:

CLI Syntax:
```
config>router
      interface interface-name
         address {[ip-address/mask]|[ip-address] [netmask]}
            [broadcast {all-ones|host-ones]
```

Configuring a Network Interface

To configure a network interface:

CLI Syntax:
```
config>router
      interface interface-name
         address ip-addr{/mask-length | mask} [broadcast {all-
            ones | host-ones}]
         egress
            filter ip ip-filter-id
         ingress
            filter ip ip-filter-id
         port port-name
```

The following displays an IP configuration output showing interface information.

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

Configuring IPv6 Parameters

IPv6 interfaces and associated routing protocols may be configured:

```
*A:7210SAS>config>system>res-prof# info
----------------------------------------------
     .....

     max-ipv6-routes1000

     ....
------------------------------------------------
```

The following displays the interface configuration showing the IPv6 default configuration when IPv6 is enabled on the interface.

```
A:ALA-49>config>router>if>ipv6# info detail
----------------------------------------------
      port 1/1/10
     ipv6
          packet-too-big 100 10
          param-problem 100 10
          redirects 100 10
          time-exceeded 100 10
          unreachables 100 10
     exit
----------------------------------------------
A:ALA-49>config>router>if>ipv6# exit all
```

Use the following CLI syntax to configure IPv6 parameters on a router interface.

CLI Syntax:
```
config>router# interface interface-name
     port port-name
     ipv6
          address {ipv6-address/prefix-length} [eui-64]
          icmp6
               packet-too-big [number seconds]
               param-problem [number seconds]
               redirects [number seconds]
               time-exceeded [number seconds]
               unreachables [number seconds]
               neighbor ipv6-address mac-address
```

The following displays a configuration example showing interface information.

```
A:ALA-49>config>router>if# info
----------------------------------------------
     address 10.11.10.1/24
     port 1/1/10
     ipv6
          address 10::1/24
     exit
```

```
----------------------------------------------
A:ALA-49>config>router>if#
```

Router Advertisement

To configure the router to originate router advertisement messages on an interface, the interface must be configured under the router-advertisement context and be enabled (no shutdown). All other router advertisement configuration parameters are optional.

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
     use-virtual-mac
```

The following displays a router advertisement configuration example.

```
*A:sim131>config>router>router-advert# info
----------------------------------------------
     interface "n1"
          prefix 3::/64
          exit
          use-virtual-mac
          no shutdown
     exit
----------------------------------------------
*A:sim131>config>router>router-advert# interface n1
*A:sim131>config>router>router-advert>if# prefix 3::/64
*A:sim131>config>router>router-advert>if>prefix# info detail
----------------------------------------------
     autonomous
     on-link
     preferred-lifetime 604800
     valid-lifetime 2592000
----------------------------------------------
*A:tahi>config>router>router-advert>if>prefix#
```

Configuring Proxy ARP

To configure proxy ARP, you can configure:

- A prefix list in the **config>router>policy-options>prefix-list** context.
- A route policy statement in the **config>router>policy-options>policy-statement** context and apply the specified prefix list.
  - → In the policy statement **entry>to** context, specify the host source address(es) for which ARP requests can or cannot be forwarded to non-local networks, depending on the specified action.
  - → In the policy statement **entry>from** context, specify network prefixes that ARP requests will or will not be forwarded to depending on the action if a match is found. For more information about route policies, refer to the Routing Protocols Guide.
- Apply the policy statement to the **proxy-arp** configuration in the **config>router>interface** context.

CLI Syntax:
```
config>router# policy-options
begin
        commit
        prefix-list name
            prefix ip-prefix/mask [exact|longer|through
            length|prefix-length-range length1-length2]
```

Use the following CLI syntax to configure the policy statement specified in the **proxy-arp-policy** *policy-statement* command.

CLI Syntax:
```
config>router# policy-options
        begin
        commit
        policy-statement name
            default-action {accept | next-entry | next-policy | reject}
            entry entry-id
                action {accept | next-entry | next-policy | reject}
                to
                    prefix-list name [name...(upto 5 max)]
                from
                    prefix-list name [name...(upto 5 max)]
```

The following displays prefix list and policy statement configuration examples:

```
A:ALA-49>config>router>policy-options# info
----------------------------------------------
    prefix-list "prefixlist1"
        prefix 10.20.30.0/24 through 32
    exit
    prefix-list "prefixlist2"
        prefix 10.10.10.0/24 through 32
    exit
...
    policy-statement "ProxyARPpolicy"
```

```
        entry 10
            from
                prefix-list "prefixlist1"
            exit
            to
                prefix-list "prefixlist2"
            exit
            action reject
        exit
        default-action accept
        exit
    exit
...
----------------------------------------------
A:ALA-49>config>router>policy-options#
```

Use the following CLI to configure proxy ARP:

CLI Syntax: `config>router>interface interface-name`
```
    local-proxy-arp
    proxy-arp-policy policy-name [policy-name...(upto 5 max)]
    remote-proxy-arp
```

The following displays a proxy ARP configuration example:

```
A:ALA-49>config>router>if# info
----------------------------------------------
    address 128.251.10.59/24
    local-proxy-arp
    proxy-arp
        policy-statement "ProxyARPpolicy"
    exit
----------------------------------------------
A:ALA-49>config>router>if#
```

Deriving the 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, then the router ID inherits the last four bytes of the MAC address. The router ID can also be manually configured in the `config>router router-id` context. On the BGP protocol level, a BGP router ID can be defined in the `config>router>bgp router-id` context and is only used within BGP.

Note that if a new router ID is configured, protocols are not automatically restarted with the new router ID. The next time a protocol is initialized the new router ID is used. An interim period of time can occur when different protocols use different router IDs. To force the new router ID, issue the `shutdown` and `no shutdown` commands for each protocol that uses the router ID, or restart the entire router.

Use the following CLI syntax to configure the router ID:

CLI Syntax:
```
config>router
  router-id router-id
  interface ip-int-name
        address {ip-address/mask | ip-address netmask} [broad-
           cast all-ones | host-ones]
```

The following example displays a router ID configuration:

```
A:ALA-4>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
        interface "system"
            address 10.10.0.4/32
        exit
     . . .
        router-id 10.10.0.4
#------------------------------------------
A:ALA-4>config>router#
```

Configuring an Autonomous System

Configuring an autonomous system is optional. Use the following CLI syntax to configure an autonomous system:

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

The following displays an autonomous system configuration example:

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

Service Management Tasks

This section discusses the following service management tasks:

- Changing the System Name on page 46
- Modifying Interface Parameters on page 47
- Deleting a Logical IP Interface on page 48

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
```

The following example displays the command usage to change the system name:

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

The following example displays the system name change:

```
A:ALA-A>config>system# name TGIF
A:TGIF>config>system# info
#------------------------------------------
# System Configuration
#------------------------------------------
        name "TGIF"
     location "Mt.View, CA, NE corner of FERG 1 Building"
     coordinates "37.390, -122.05500 degrees lat."
     synchronize
     snmp
        exit
        security
            snmp
                community "private" rwa version both
            exit
        exit
        . . .
----------------------------------------------
A:TGIF>config>system#
```

Modifying Interface Parameters

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

To modify an IP address, perform the following steps:

Example:
```
A:ALA-A>config>router# interface “to-sr1”
A:ALA-A>config>router>if# shutdown
A:ALA-A>config>router>if# no address
A:ALA-A>config>router>if# address 10.0.0.25/24
A:ALA-A>config>router>if# no shutdown
```

To modify a port, perform the following steps:

Example:
```
A:ALA-A>config>router# interface “to-sr1”
A:ALA-A>config>router>if# shutdown
A:ALA-A>config>router>if# no port
A:ALA-A>config>router>if# port 1/1/2
A:ALA-A>config>router>if# no shutdown
```

The following example displays the interface configuration:

```
A:ALA-A>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
        interface "system"
            address 10.0.0.103/32
        exit
        interface "to-sr1"
            address 10.0.0.25/24
            port 1/1/2
        exit
        router-id 10.10.0.3
#------------------------------------------
A:ALA-A>config>router#
```

Deleting a Logical IP Interface

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

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

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

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

IP Router Command Reference

Command Hierarchies

Configuration Commands

- Router Commands on page 50
- Router Interface Commands on page 51
- Router Interface IPv6 Commands on page 51
- Router Advertisement Commands on page 53
- Show Commands on page 54
- Clear Commands on page 55

Router Commands

config
- — **router** [*router-name*]
  - — **aggregate** *ip-prefix/ip-prefix-length* **[summary-only]**
  - — **no aggregate** *ip-prefix/ip-prefix-length*
  - — **autonomous-system** *autonomous-system*
  - — **no autonomous-system**
  - — **router-id** *ip-address*
  - — **no router-id**
  - — [**no**] **static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**enable** | **disable**] **next-hop** *gateway* [bfd-enable]
  - — [**no**] **triggered-policy**

Router Interface Commands

config
— **router** [*router-name*]
— [**no**] **interface** *ip-int-name*
— **accounting-policy** *policy-id*
— **no accounting-policy**
— **address** {*ip-address/mask* | *ip-address netmask*} [**broadcast** {**all-ones** | **host-ones**}]
— **no address**[**no**] **allow-directed-broadcasts**
— **arp-timeout** *seconds*
— **no arp-timeout**
— **bfd** *transmit-interval* [**receive** *receive-interval*] [**multiplier** *multiplier*] [**echo-receive** *echo-interval*
— **no bfd**
— **delayed-enable**
— **no delayed-enable**
— **description** *long-description-string*
— **no description**
— **egress**
— **filter ip** *ip-filter-id*
— **filter ipv6** *ipv6-filter-id*
— **no filter [ip** *ip-filter-id*] **[ipv6** *ipv6-filter-id*]
— **icmp**
— [**no**] **mask-reply**
— **redirects** [*number seconds*]
— **no redirects**
— **ttl-expired** [*number seconds*]
— **no ttl-expired**
— **unreachables** [*number seconds*]
— **no unreachables**
— **ingress**
— **filter ip** *ip-filter-id*
— **no filter**
— **[no] filter ipv6** *ipv6-filter-id*
— **ldp-sync-timer** *seconds*
— **no ldp-sync-timer**
— **[no] local-proxy-arp**
— [**no**] **loopback**
— **mac** *ieee-mac-addr*
— **no mac**
— [**no**] **ntp-broadcast**
— **port** *port-name*
— **no port**
— **[no] proxy-arp-policy** *policy-name [policy-name...(upto 5 max)]*
— **[no] remote-proxy-arp**
— [**no**] **shutdown**
— **static-arp** *ip-address ieee-address*
— **no static-arp** *ip-address*
— **tos-marking-state** {**trusted** | **untrusted**}
— **no tos-marking-state**

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*
    - — **icmp6**
      - — **packet-too-big** [*number seconds*]
      - — **no packet-too-big**
      - — **param-problem** [*number seconds*]
      - — **no param-problem**
      - — **redirects** [*number seconds*]
      - — **no redirects**
      - — **time-exceeded** *number seconds*]
      - — **no time-exceeded**
      - — **unreachables** [*number seconds*]
      - — **no unreachables**
    - — [**no**] **local-proxy-nd**
    - — **neighbor** *ipv6-address* [*mac-address*]
    - — **no neighbor** *ipv6-address*
    - — **proxy-nd-policy** *policy-name* [*policy-name*...(up to 5 max)]
    - — **no proxy-nd-policy**

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**
— [**no**] **autonomous**
— [**no**] **on-link**
— **preferred-lifetime** {*seconds* | **infinite**}
— **no preferred-lifetime**
— **valid-lifetime**{*seconds* | **infinite**}
— **no valid-lifetime**
— **reachable-time** *milli-seconds*
— **no reachable-time**
— **retransmit-time** *milli-seconds*
— **no retransmit-time**
— **router-lifetime** *seconds*
— **no router-lifetime**
— [**no**] **shutdown**

Show Commands

show
— **router** *router-instance*
— **aggregate** [*active*]
— **arp** [*ip-int-name* | *ip-address/mask* | **mac** *ieee-mac-address* | **summary**] [**local** | **dynamic** | **static** | **managed**]
— **bfd**
— **interface** [*interface-name*]
— **session** [**src** *ip-address* [**dst** *ip-address*] | [**detail**]]
— **fib** *slot-number* [*ip-prefix/prefix-length* [*longer*]]
— **interface** [{[*ip-address* | *ip-int-name*] [**detail**]} | [**summary**]
— **icmp6**
— **interface** [*interface-name*]
— **interface** [{[*ip-address* | *ip-int-name*] [**detail**] [*family*]} | [**summary**] | [**exclude-services**]
— **interface** *family* [**detail**]
— **interface** *ip-address* | *ip-int-name*> **stastistics**
— **neighbor** *family* [*ip-address* | *ip-int-name* | **mac** *ieee-mac-address* | **summary**]
— **policy** [*name* | **prefix-list** [**name**] | **admin**]
— **route-table** [*family* [*ip-prefix* [*prefix-length*] [**longer**|**exact**]| [**protocol** *protocol-name* | [**summary**]
— **rtr-advertisement** [**interface** *interface-name*] [**prefix** *ipv6-prefix[/prefix-length*] [**conflicts**]
— **static-arp** [*ip-address* | *ip-int-name* | **mac** *ieee-mac-addr*]
— **static-route** [family] [[*ip-prefix /mask*] [*ip-prefix /prefix-length*] | [**preference** *preference*] | [**next-hop** *ip-address*] | [**detail**]
— **status**
— **tunnel-table** [*ip-address*[/*mask*]] | [**protocol** *protocol* | **sdp** *sdp-id*] [**summary**]

Clear Commands

clear
- — **router** [*router-instance*]
  - — **arp** {**all** | *ip-addr* | **interface** {*ip-int-name* | *ip-addr*}}
  - — **bfd**
    - — **session src-ip** *ip-address* **dst-ip** *ip-address*
    - — **statistics src-ip** *ip-address* **dst-ip** *ip-address*
    - — **statistics all**
  - — **icmp6 all**
  - — **icmp6 global**
  - — **icmp6 interface** *interface-name*
  - — **neighbor** {**all** | *ipv6-address*}
  - — **neighbor interface** [*ip-int-name* | **interface** *interface-name*]
  - — **router-advertisement all**
  - — **router-advertisement** [**interface** *interface-name*]

Debug Commands

debug
- — **router** *router-instance*
  - — **ip**
    - — [**no**] **arp**
    - — **icmp**
    - — **no icmp**
    - — **icmp6** [*ip-int-name*]
    - — **no icmp6**
    - — [**no**] **interface** [*ip-int-name* | *ip-address*]
    - — **neighbor** [*ip-int-name*]
    - — **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**

Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context config>router>interface
config>router>router-advertisement

Description The **shutdown** command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

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

description

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

Context config>router>if

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

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

Default No description is associated with the configuration context.

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

Router Global Commands

router

Syntax **router**

Context config

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

aggregate

Syntax **aggregate** *ip-prefix/ip-prefix-length* [**summary-only**]
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 (BGP, IS-IS or OSPF) such as the route type, or OSPF tag, to aggregate routes.

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

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

Default No aggregate routes are defined.

Parameters *ip-prefix/ip-prefix-length* — The destination address of the aggregate route in dotted decimal notation.

Values

ipv4-prefix	a.b.c.d (host bits must be 0)	
ipv4-prefix-length	0 — 32ipv6-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 — FFFF]H	
	d: [0 — 255]D	
ipv6-prefix-length	0 — 128	

The mask associated with the network address expressed as a mask length.

Values 0 — 32

summary-only — This optional parameter 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.

autonomous-system

Syntax **autonomous-system** *autonomous-system*
no autonomous-system

Context config>router

Description This command configures the autonomous system (AS) number for the router. A router can only belong to one AS. An AS number is a globally unique number with an AS. This number is used to exchange exterior routing information with neighboring ASs and as an identifier of the AS itself.

If the AS number is changed on a router with an active BGP instance, the new AS number is not used until the BGP instance is restarted either by administratively disabling/enabling (**shutdown**/ **no shutdown**) the BGP instance or rebooting the system with the new configuration.

Default No autonomous system number is defined.

Parameters *autonomous-system* — The autonomous system number expressed as a decimal integer.

Values 1 — 4294967295

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 both OSPF and BGP routing protocols in this instance of the routing table manager. IS-IS uses the router ID value as its system ID.

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 of time 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 to 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, use the last 32 bits of the chassis MAC address.

Parameters *router-id* — The 32 bit router ID expressed in dotted decimal notation or as a decimal value.

triggered-policy

Syntax **triggered-policy**
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. There may be circumstances when the changes should or must be delayed; for example, if a policy change is implemented that would affect every BGP peer on a 7210 SAS M, X router, the consequences could be dramatic. It would be 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, 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. This keeps the peer up, and the change made to a route policy is applied only to that peer or group of peers.

static-route

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

[**no**] **static-route** {*ip-prefix/prefix-length* **|** *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**enable | disable**] **black-hole**

Context config>router

Description This command creates static route entries for both the network and access routes.
When configuring a static route, either **next-hop** or **black-hole** must be configured.
The **no** form of the command deletes the static route entry. If a static route needs to be removed when multiple static routes exist to the same destination, then as many parameters to uniquely identify the static route must be entered.

Default No static routes are defined.

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

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

ip-address — The IP address of the IP interface. The *ip-addr* 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 ipv4-address a.b.c.d (host bits must be 0)ipv6-addressx:x:x:x:x:x:x:x[-interface]

x:x:x:x:x:x:d.d.d.d[-interface]
x: [0..FFFF]H
d: [0..255]D

netmask — The subnet mask in dotted decimal notation.

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

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

Different protocols should not be configured with the same preference. If this occurs, the tiebreaker is according to the default preference table defined in Table 4 on page 62.

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, then the route to use is determined by the next-hop with the lowest address.

Values 1 — 255

metric *metric* **—** The cost metric for the static route, expressed as a decimal integer. When modifying the metric of an existing static route, the preference will not change unless specified. This value is also used to determine which static route to install in the forwarding table:

- If there are multiple static routes with the same preference but different metrics then the lower cost (metric) route will be installed.
- If there are multiple static routes with equal preferences and metrics the route with the lowest next-hop will be installed .
- If there are multiple routes with different preferences then the lower preference route will be installed.

Default 1

Values 0 — 65535

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

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

The *gateway* configured here can be either on the network side or the access side on this node. This address must be associated with a network directly connected to a network configured on this node.

Values ip-int-name 32 chars max
black-hole

Specifies the route is a black hole route. If the destination address on a packet matches this static route, it will be silently discarded.

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

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

Table 4: Default Route Preferences

Route Type	Preference	Configurable
Direct attached	0	No
Static-route	5	Yes
OSPF Internal routes	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

Default 5

Values 1 — 4294967295

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

The administrative state is maintained in the configuration file.

Default enable

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

The administrative state is maintained in the configuration file.

Default enable

bfd-enable — This parameter is supported on 7210 SAS M, X devices configured in Network mode. It associates the state of the static route to a BFD session between the local system and the configured nexthop. This keyword cannot be configured if the nexthop is **indirect** or **blackhole** keywords are specified.

Router Interface Commands

interface

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

Context config>router

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

Interface names are case-sensitive and must be unique within the group of IP interfaces defined for **config router interface**. Interface names must not be in the dotted decimal notation of an IP address.; 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 as an IP address and an interface name.

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 ip-int-name "**system**" is associated with the network entity (such as a specific 7210 SAS M), not a specific interface. The system interface is also referred to as the loopback address.

The **no** form of the command removes the IP interface and all the associated configurations. The interface must be administratively shut down before issuing the **no interface** command.

Default No interfaces or names are defined within the system.

Parameters *ip-int-name* — The name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 1 — 32 alphanumeric characters.

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

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context config>router

Description An accounting policy must be defined before it can be associated with a SAP. If the policy-id does not exist, an error message is generated. A maximum of one accounting policy can be associated with a SAP at one time.

Default Default accounting policy

Parameters *acct-policy-id* — Enter the accounting policy-id as configured in the config>router>accounting-policycontext.

Values 1 — 99

address

Syntax **address** {*ip-address*/*mask* | *ip-address netmask*} [**broadcast** {**all-ones** | **host-ones**}]
no address

Context config>router>interface

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

An IP address must be assigned to each IP interface. An IP address and a mask combine to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the router.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. **Show** commands display CIDR notation and are stored in configuration files.

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

The **no** form of the command removes the IP address assignment from the IP interface. The **no** form of this command can only be performed when the IP interface is administratively shut down. Shutting down the IP interface will operationally stop any protocol interfaces or MPLS LSPs that explicitly reference that IP address. When a new IP address is defined, the IP interface can be administratively enabled (**no shutdown**), which reinitializes the protocol interfaces and MPLS LSPs associated with that IP interface.

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

Default No IP address is assigned to the IP interface.

Parameters *ip-address* — The IP address of the IP interface. The *ip-addr* 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 — 223.255.255.255

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

mask-length — 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-addr* from the *mask-length* parameter. The mask length 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. Allowed values are integers in the range 1— 32. Note that a mask length of 32 is reserved for system IP addresses.

Values 1 — 32

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-addr* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that will be used in a logical 'AND' function to derive the local subnet of the IP address. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

Values 128.0.0.0 — 255.255.255.255

netmask — The subnet mask in dotted decimal notation.

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

broadcast {**all-ones** | **host-ones**} **—** The optional **broadcast** parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is **host-ones,** which indictates a subnet broadcast address. Use this parameter to change the broadcast address to **all-ones** or revert back to a broadcast address of **host-ones**.

The **all-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

The **host-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-addr* and the *mask-length* or *mask* with all the host bits set to binary 1. This is the default broadcast address used by an IP interface.

The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed.

This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (**all-ones**) or the valid subnet broadcast address (**host-ones**) will be received by the IP interface.

Default host-ones

Values **all-ones**, **host-ones**

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 to the subnet broadcast address of the egress IP interface.

When enabled, a frame destined to the local subnet on this IP interface is sent as a subnet broadcast out this interface. **NOTE**: Allowing directed broadcasts is a well-known mechanism used for denial-of-service attacks.

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

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

Default no allow-directed-broadcasts — Directed broadcasts are dropped.

arp-timeout

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

Context config>router>interface

Description This command configures the minimum time, in seconds, an ARP entry learned on the IP interface is stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host. Otherwise, the ARP entry is aged from the ARP table. If the **arp-timeout** value is set to 0 seconds, ARP aging is disabled.

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

Default 14400 seconds (4 hours)

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 — 65535

bfd

Syntax **bfd** *transmit-interval* [**receive** *receive-interval*] [**multiplier** *multiplier*] [**echo-receive** *echo-interval*]
no bfd

Context config>router>interface

Description This command specifies the bi-directional forwarding detection (BFD) parameters for the associated IP interface. If no parameters are defined the default values are used.

The multiplier specifies the number of consecutive BFD messages that must be missed from the peer before the BFD session state is changed to down and the upper level protocols (OSPF, IS-IS) is notified of the fault.

The **no** form of the command removes BFD from the router interface regardless of the RSVP.

Important notes: On the 7210 SAS, the *transmit-interval* and **receive *receive-interval*** values can only be modified to a value less than 100 ms when:

1. The service is shut down (**shutdown**)
2. The interval is specified 100 — 100000.
3. The service is re-enabled (**no shutdown**)

Default no bfd

Parameters *transmit-interval* — Sets the transmit interval, in milliseconds, for the BFD session.

Values 100 — 100000

Default 100

receive *receive-interval* — Sets the receive interval, in milliseconds, for the BFD session.

Values 100 — 100000

Default 100

multiplier *multiplier* — Set the multiplier for the BFD session.

Values 3— 20

Default 3

echo-receive *echo-interval* **—** Sets the minimum echo receive interval, in milliseconds, for the session.

Values 100 — 100000

Default 100

delayed-enable

Syntax ***delayed-enable seconds***
no *delayed-enable*

Context config>router>interface

Description This command creates a delay to make the interface operational by the specified number of seconds

The value is used whenever the system attempts to bring the interface operationally up.

Parameters *seconds* — Specifies a delay, in seconds, to make the interface operational.

Values 1 — 1200

ldp-sync-timer

Syntax **ldp-sync-timer** *seconds*
no ldp-sync-timer

Context config>router>interface

Description This command enables synchronization of IGP and LDP. When a link is restored after a failure, IGP sets the link cost to infinity and advertises it. The actual value advertised in OSPF is 0xFFFF (65535). The actual value advertised in IS-IS regular metric is 0x3F (63) and in IS-IS wide-metric is 0xFFFFFE (16777214). This feature is not supported on RIP interfaces.

Note that if an interface belongs to both IS-IS and OSPF, a physical failure will cause both IGPs to advertise infinite metric and to follow the IGP-LDP synchronization procedures. If only one IGP bounced on this interface or on the system, then only the affected IGP advertises the infinite metric and follow the IGP-LDP synchronization procedures.

Next LDP hello adjacency is brought up with the neighbour. The LDP synchronization timer is started by IGP from the time the LDP session to the neighbor is UP over the interface. This is to allow time for the label-FEC bindings to be exchanged.

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

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 expired. Also, the new cost value will be advertised after the user executes any of the following commands if the currently advertised cost is different:

- tools>perform>router>isis>ldp-sync-exit
- tools>perform>router>ospf>ldp-sync-exit
- config>router>interface>no ldp-sync-timer
- config>router>ospf>disable-ldp-sync
- router>isis>disable-ldp-sync

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, then 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, it will only consider this interface for forwarding after IGP re-advertized its actual cost value.

Note that the LDP Sync Timer State is not always synched across to the standby CPM, so after an activity switch the timer state might not be same as it was on the previous active CPM.

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

Default no ldp-sync-timer

Parameters *seconds* — Specifies the time interval for the IGP-LDP synchronization timer in seconds.

Values 1 – 1800

local-proxy-arp

Syntax **[no] local-proxy-arp**

Context config>router>interface

Description This command enables local proxy ARP on the interface.

Default no local-proxy-arp

loopback

Syntax [**no**] **loopback**

Context config>router>interface

Description This command configures the interface as a loopback interface.

Default Not enabled

mac

Syntax **mac** *ieee-mac-addr*
no mac

Context config>router>interface

Description This command assigns a specific MAC address to an IP interface. Only one MAC address can be assigned to an IP interface. When multiple **mac** commands are entered, the last command overwrites the previous command.

The **no** form of the command returns the MAC address of the IP interface to the default value.

Default IP interface has a system-assigned MAC address.

Parameters *ieee-mac-addr* — Specifies the 48-bit MAC address for the IP interface 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.

ntp-broadcast

Syntax [**no**] **ntp-broadcast**

Context config>router>interface

Description This command enables SNTP broadcasts received 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 re-attempted. The *port-id* can be in one of the following forms:

- Ethernet Interfaces

  If the card in the slot has MDAs, *port-id* is in the slot_number/MDA_number/port_number format; for example, **1/1/3** specifies port 3 of the MDA installed in MDA slot 1 on the card installed in chassis slot 1.

  The encapsulation type is an property of a Ethernet network port. The port in this context can be tagged with either IEEE 802.1Q (referred to as dot1q) encapsulation or null encapsulation. Dot1q encapsulation supports multiple logical IP interfaces on a given network port and Null encapsulation supports a single IP interface on the network port.

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

Default No port is associated with the IP interface.

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

Values

port-name	*port-id* [:encap-val]	
encap-val	- 0	for null
	- [0..4094]	for dot1q
port-id:	slot/mda/port[.channel]	
lag-id	- lag-<id>	
lag	- keyword	
id	- [1..200]	

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 queue-redirect-group parameter creates an association between the IP interface and an egress port queue group. When the network QoS policy ID contains an egress forwarding plane that is directed to a queue group queue ID, the network QoS policy must be applied to the IP interface with a valid egress port queue group name. The queue group name must exist on the egress port associated with the IP interface and the group must contain a queue ID matching the queue ID for each redirected forwarding class in the QoS policy.

The IP interface may redirect its forwarding classes to a single port queue group. Forwarding classes that are not redirected to a queue within the group are mapped to the default forwarding class egress queue on the port.

If the QoS command is re-executed without the queue-redirect-group parameter specified, all forwarding classes will be remapped to the default port forwarding class egress queues.

The **no** form of the command removes the QoS policy association from the SAP or 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* — An existing network policy ID to associate with the IP interface.

Values 1 — 65535

queue-redirect-group *queue-group-name* **—** This optional parameter specifies that the *queue-group-name* will be used for all egress forwarding class redirections within the network QoS policy ID. The specified *queue-group-name* must exist as a port egress queue group on the port associated with the IP interface.

proxy-arp-policy

Syntax **[no] proxy-arp-policy** *policy-name [policy-name...(up to 5 max)]*

Context config>router>interface

Description This command enables and configures proxy ARP on the interface and specifies an existing policystatement to analyze match and action criteria that controls the flow of routing information to and from a given protocol, set of protocols, or a particular neighbor. The policy-name is configured in the config>router>policy-options context.

Use proxy ARP so the 7210 SAS responds to ARP requests on behalf of another device. Static ARP is used when a 7210 SAS needs to know about a device on an interface that cannot or does not respond to ARP requests. Thus, the 7210 SAS configuration can state that if it has a packet that has a certain IP address to send it to the corresponding ARP address.

Default no proxy-arp-policy

Parameters *policy-name* — The export route policy 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, and so on), the entire string must be enclosed within double quotes. The specified policy name(s) must already be defined.

remote-proxy-arp

Syntax **[no] remote-proxy-arp**

Context config>router>interface

Description This command enables remote proxy ARP on the interface.

Default no remote-proxy-arp

static-arp

Syntax **static-arp** *ip-addr ieee-mac-addr*
no static-arp *ip-addr*

Context config>router>interface

Description This command configures a static Address Resolution Protocol (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.
The number of static-arp entries that can be configured on a single node is limited to 1000.
Static ARP is used when a 7210 SAS M needs to know about a device on an interface that cannot or does not respond to ARP requests. Thus, the 7210 SAS M OS configuration can state that if it has a packet that has a certain IP address to send it to the corresponding ARP address. Use proxy ARP so the 7210 SAS M, X responds to ARP requests on behalf of another device.

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

Default No static ARPs are defined.

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

ieee-mac-addr — Specifies 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.

tos-marking-state

Syntax **tos-marking-state** {**trusted** | **untrusted**}
no tos-marking-state

Context config>router>interface

Description This command is used on a network IP interface to alter the default trusted state to a non-trusted state. When unset or reverted to the trusted default, the ToS field will not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set, in which case the egress network interface treats all IES and network IP interface as untrusted.

When the ingress network IP interface is set to untrusted, all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface. The egress network remarking rules also apply to the ToS field of IP packets routed using IGP shortcuts (tunneled to a remote next-hop). However, the tunnel QoS markings are always derived from the egress network QoS definitions.

Egress marking and remarking is based on the internal forwarding class and profile state of the packet once it reaches the egress interface. The forwarding class is derived from ingress classification functions. The profile of a packet is either derived from ingress classification or ingress policing.

The default marking state for network IP interfaces is trusted. This is equivalent to declaring no tos-marking-state on the network IP interface. When undefined or set to tos-marking-state trusted, the trusted state of the interface will not be displayed when using show config or show info unless the detail parameter is given. The **save config** command will not store the default tos-marking-state trusted state for network IP interfaces unless the detail parameter is also specified.

The **no** tos-marking-state command is used to restore the trusted state to a network IP interface. This is equivalent to executing the tos-marking-state trusted command.

Default trusted

Parameters **trusted —** The default prevents the ToS field to not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set

untrusted — Specifies that all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface.

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 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 is not defined, no filtering is performed.

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
no filter

Context config>router>if>ingress
config>router>if>egress

Description This command associates an IP filter policy with an IP interface.

Filter policies control packet forwarding and dropping based on IP match criteria.

The *ip-filter-id* must have been pre-configured before this **filter** command is executed. If the filter ID does not exist, an error occurs.

Only one filter ID can be specified.

The **no** form of the command removes the filter policy association with the IP interface.

Default No filter is specified.

Parameters **ip** *ip-filter-id* — The filter name acts as the ID for the IP filter policy expressed as a decimal integer. The filter policy must already exist within the **config>filter>ip** context.

Values 1 — 65535

ipv6 *ipv6-filter-id* — The filter name acts as the ID for the IPv6 filter policy expressed as a decimal integer. The filter policy must already exist within the **config>filter>ip** context.

Values 1 — 65535

Router Interface ICMP Commands

icmp

Syntax **icmp**

Context config>router>interface

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

mask-reply

Syntax [**no**] **mask-reply**

Context config>router>if>icmp

Description This command enables 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.

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context config>router>if>icmp

Description This command enables and configures the rate for ICMP redirect messages issued on the router interface.

When routes are not optimal on this router, and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The **redirects** command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects are issued can be controlled with the optional *number* and *time* parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.

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

The **no** form of the command disables the generation of ICMP redirects on the router interface.

Default redirects 100 10 — Maximum of 100 redirect messages in 10 seconds.

Parameters *number* — The maximum number of ICMP redirect messages to send, expressed as a decimal integer. This parameter must be specified with the *time* parameter.

Values 10 — 1000

seconds — The time frame, in seconds, used to limit the *number* of ICMP redirect messages that can be issued,expressed as a decimal integer.

Values 1 — 60

ttl-expired

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

Context config>router>if>icmp

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

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

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

Default ttl-expired 100 10 — Maximum of 100 TTL expired message in 10 seconds.

Parameters *number* — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. The *seconds* parameter must also be specified.

Values 10 — 1000

seconds — The time frame, in seconds, used to limit the *number* of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

Values 1 — 60

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context config>router>if>icmp

Description This command enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of destination unreachable messages that can be issued on the interface for a given time interval.

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

The **no** form of the command disables the generation of ICMP destination unreachables on the router interface.

Default unreachables 100 10 — Maximum of 100 unreachable messages in 10 seconds.

Parameters *number* — The maximum number of ICMP unreachable messages to send, expressed as a decimal integer. The *seconds* parameter must also be specified.

Values 10 — 1000

seconds — The time frame, in seconds, used to limit the *number* of ICMP unreachable messages that can be issued, expressed as a decimal integer.

Values 1— 60

Router Interface IPv6 Commands

ipv6

Syntax [**no**] **ipv6**

Context config>router>interface

Description This command configures IPv6 for a router interface.

The **no** form of the command disables IPv6 on the interface.

Default not enabled

address

Syntax **address** {*ipv6-address/prefix-length*} [**eui-64**]
no address {*ipv6-address/prefix-length*}

Context config>router>if>ipv6

Description This command assigns an IPv6 address to the interface.

Default none

Parameters *ipv6-address/prefix-length* — Specify the IPv6 address on the interface.

Values	ipv6-address/prefix: 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 — FFFF]H d [0 — 255]D
	prefix-length	1 — 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. The 64-bit interface identifier is derived from MAC address on Ethernet interfaces. For interfaces without a MAC address, for example POS interfaces, the Base MAC address of the chassis should be used.

icmp6

Syntax **icmp6**

Context config>router>if>ipv6

Description This command enables the context to configure ICMPv6 parameters for the interface.

packet-too-big

Syntax **packet-too-big** [*number seconds*]
no packet-too-big

Context config>router>if>ipv6>icmp6

Description This command configures the rate for ICMPv6 packet-too-big messages.

Parameters *number* — Limits the number of packet-too-big messages issued per the time frame specifed in the *seconds* parameter.

Values 10 — 1000

seconds — Determines the time frame, in seconds, that is used to limit the number of packet-too-big messages issued per time frame.

Values 1 — 60

param-problem

Syntax **param-problem** [*number seconds*]
no param-problem

Context config>router>if>ipv6>icmp6

Description This command configures the rate for ICMPv6 param-problem messages.

Parameters *number* — Limits the number of param-problem messages issued per the time frame specifed in the *seconds* parameter.

Values 10 — 1000

seconds — Determines the time frame, in seconds, that is used to limit the number of param-problem messages issued per time frame.

Values 1 — 60

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context config>router>if>ipv6>icmp6

Description This command configures the rate for ICMPv6 redirect messages. When configured, ICMPv6 redirects are generated when routes are not optimal on the router and another router on the same subnetwork has a better route to alert that node that a better route is available.

The **no** form of the command disables ICMPv6 redirects.

Default 100 10 (when IPv6 is enabled on the interface)

Parameters *number* — Limits the number of redirects issued per the time frame specifed in *seconds* parameter.

Values 10 — 1000

seconds — Determines the time frame, in seconds, that is used to limit the number of redirects issued per time frame.

Values 1 — 60

time-exceeded

Syntax **time-exceeded** [*number seconds*]
no time-exceeded

Context config>router>if>ipv6>icmp6

Description This command configures rate for ICMPv6 time-exceeded messages.

Parameters *number* — Limits the number of time-exceeded messages issued per the time frame specifed in *seconds* parameter.

Values 10 — 1000

seconds — Determines the time frame, in seconds, that is used to limit the number of time-exceeded messages issued per time frame.

Values 1 — 60

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context config>router>if>ipv6>icmp6

Description This command configures the rate for ICMPv6 unreachable messages. When enabled, ICMPv6 host and network unreachable messages are generated by this interface.

The **no** form of the command disables the generation of ICMPv6 host and network unreachable messages by this interface.

Default 100 10 (when IPv6 is enabled on the interface)

Parameters *number* — Determines the number destination unreachable ICMPv6 messages to issue in the time frame specified in *seconds* parameter.

Values 10 — 1000

seconds — Sets the time frame, in seconds, to limit the number of destination unreachable ICMPv6 messages issued per time frame.

Values 1 — 60

link-local-address

Syntax **link-local-address** *ipv6-address* [**preferred**]
no link-local-address

Context config>router>if>ipv6

Description This command configures the link local address.

local-proxy-nd

Syntax [**no**] **local-proxy-nd**

Context config>router>if>ipv6

Description This command enables local proxy neighbor discovery on the interface.

The **no** form of the command disables local proxy neighbor discovery.

proxy-nd-policy

Syntax **proxy-nd-policy** *policy-name* [*policy-name*...(up to 5 max)]
no proxy-nd-policy

Context config>router>if>ipv6

Description This command configure a proxy neighbor discovery policy for the interface.

Parameters *policy-name* — The neighbor discovery policy 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 specified policy name(s) must already be defined.

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 for some reason, a static address must be used. This command can only be used on Ethernet media.

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 assigned to a router 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 — FFFF]H
d: [0 — 255]D

mac-address — Specifies the MAC address for the neighbor in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Router Advertisement Commands

router-advertisement

Syntax [**no**] **router-advertisement**

Context config>router

Description This command configures router advertisement properties. By default, it is disabled for all IPv6 enabled interfaces.

The **no** form of the command disables all IPv6 interface. However, the **no interface** *interface-name* command disables a specific interface.

Default disabled

interface

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

Context config>router>router-advertisement

Description This command configures router advertisement properties on a specific interface. The interface must already exist in the **config>router>interface** context.

Default No interfaces are configured by default.

Parameters *ip-int-name* — Specify the interface name. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

current-hop-limit

Syntax **current-hop-limit** *number*
no current-hop-limit

Context config>router>router-advert>if

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 packets.

Default 64

Parameters *number* — Specifies the hop limit.

Values 0 — 255. A value of zero means there is an unspecified number of hops.

managed-configuration

Syntax [**no**] **managed-configuration**

Context config>router>router-advert>if

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. .

Default no managed-configuration

max-advertisement-interval

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

Context config>router>router-advert>if

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

Default 600

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

Values 4 — 1800

min-advertisement-interval

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

Context config>router>router-advert>if

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

Default 200

Parameters *seconds* — Specify the minimum interval in seconds between sending ICMPv6 neighbor discovery router advertisement messages.

Values 3 — 1350

mtu

Syntax [**no**] **mtu** *mtu-bytes*

Context config>router>router-advert>if

Description This command configures the MTU for the nodes to use to send packets on the link.

Default no mtu — The MTU option is not sent in the router advertisement messages.

Parameters *mtu-bytes* — Specify the MTU for the nodes to use to send packets on the link.

Values 1280 — 9212

other-stateful-configuration

Syntax [**no**] **other-stateful-configuration**

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. .

Default no other-stateful-configuration

prefix

Syntax [**no**] **prefix** [*ipv6-prefix*/*prefix-length*]

Context config>router>router-advert>if

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 explicitly configured using prefix statements.

Default none

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

Values	ipv4-prefix	a.b.c.d (host bits must be 0)	
	ipv4-prefix-length	0 — 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 — FFFF]H
		d:	[0 — 255]D
	ipv6-prefix-length	0 — 128	

prefix-length — Specifies a route must match the most significant bits and have a prefix length.

Values 1 — 128

autonomous

Syntax [**no**] **autonomous**

Context config>router>router-advert>if>prefix

Description This command specifies whether the prefix can be used for stateless address autoconfiguration.

Default enabled

on-link

Syntax [**no**] **on-link**

Context config>router>router-advert>if>prefix

Description This command specifies whether the prefix can be used for onlink determination.

Default enabled

preferred-lifetime

Syntax [**no**] **preferred-lifetime** {*seconds* | **infinite**}

Context config>router>router-advert>if

Description This command configures the remaining length of time in seconds that this prefix will continue to be preferred, such as, time until deprecation. The address generated from a deprecated prefix should not be used as a source address in new communications, but packets received on such an interface are processed as expected.

Default 604800

Parameters *seconds* — Specifies the remaining length of time in seconds that this prefix will continue to be preferred.

infinite — Specifies that the prefix will always be preferred. A value of 4,294,967,295 represents infinity.

valid-lifetime

Syntax **valid-lifetime** {*seconds* | **infinite**}

Context config>router>router-advert>if

Description This command specifies the length of time in seconds that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity.

The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

Default 2592000

Parameters *seconds* — Specifies the remaining length of time in seconds that this prefix will continue to be valid.

infinite — Specifies that the prefix will always be valid. A value of 4,294,967,295 represents infinity.

reachable-time

Syntax **reachable-time** *milli-seconds*
no reachable-time

Context config>router>router-advert>if

Description This command configures how long this router should be considered reachable by other nodes on the link after receiving a reachability confirmation.

Default no reachable-time

Parameters *milli-seconds* — Specifies the length of time the router should be considered reachable.

Values 0 — 3600000

retransmit-time

Syntax **retransmit-timer** *milli-seconds*
no retransmit-timer

Context config>router>router-advert>if

Description This command configures the retransmission frequency of neighbor solicitation messages.

Default no retransmit-time

Parameters *milli-seconds* — Specifies how often the retransmission should occur.

Values 0 — 1800000

router-lifetime

Syntax **router-lifetime** *seconds*
no router-lifetime

Context config>router>router-advert>if

Description This command sets the router lifetime.

Default 1800

Parameters *seconds* — The length of time, in seconds, (relative to the time the packet is sent) that the prefix is valid for route determination.

Values 0, 4 — 9000 seconds. 0 means that the router is not a default router on this link.

Show Commands

aggregate

Syntax **aggregate** [**active**]

Context show>router

Description This command displays aggregate routes.

Parameters **active —** When the active keyword is specified, inactive aggregates are filtered out.

arp

Syntax **arp** [*ip-int-name* **|** *ip-address/mask* **| mac** *ieee-mac-address* **| summary**] [**local | dynamic | static**]

Context show>router

Description This command displays the router ARP table sorted by IP address. If no command line options are specified, all ARP entries are displayed.

Parameters *ip-address/mask* — Only displays ARP entries associated with the specified IP address and mask.

ip-int-name — Only displays ARP entries associated with the specified IP interface name.

mac *ieee-mac-addr* **—** Only displays ARP entries associated with the specified MAC address.

summary — Displays an abbreviate list of ARP entries.

[**local** | **dynamic** | **static**] — Only displays ARP information associated with the keyword.

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

Label	Description
`IP Address`	The IP address of the ARP entry.
`MAC Address`	The MAC address of the ARP entry.
`Expiry`	The age of the ARP entry.
`Type`	`Dyn` — The ARP entry is a dynamic ARP entry. `Inv` — The ARP entry is an inactive static ARP entry (invalid). `Oth` — The ARP entry is a local or system ARP entry. `Sta` — The ARP entry is an active static ARP entry.
`*Man`	The ARP entry is a managed ARP entry.
`Int`	The ARP entry is an internal ARP entry.

Label	Description (Continued)
[I}	The ARP entry is in use.
Interface	The IP interface name associated with the ARP entry.
No. of ARP Entries	The number of ARP entries displayed in the list.

Sample Output

```
*B:7710-Red-RR# show router arp
===============================================================================
ARP Table (Router: Base)
===============================================================================
IP Address      MAC Address       Expiry    Type   Interface
-------------------------------------------------------------------------------
10.20.1.24      00:16:4d:23:91:b8 00h00m00s Oth    system
10.10.4.11      00:03:fa:00:d0:c9 00h57m03s Dyn[I] to-core-sr1
10.10.4.24      00:03:fa:41:8d:20 00h00m00s Oth[I] to-core-sr1
-------------------------------------------------------------------------------
No. of ARP Entries: 3
===============================================================================


A:ALA-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:ALA-A#


A:ALA-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    Dyn  to-ser1
===============================================================================
A:ALA-A#
```

bfd

Syntax **bfd**

Context show>router

Description This command enables the context to display bi-directional forwarding detection (BFD) information.

interface

Syntax **interface** *[interface-name*]

Context show>router>bfd

Description This command displays interface information.

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

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

Sample Output

```
*A:7210-SAS>show>router>bfd# interface
===============================================================================
BFD Interface
===============================================================================
Interface name                     Tx Interval    Rx Interval    Multiplier
-------------------------------------------------------------------------------
F_Port                             100            100            3
F_Lag                              300            300            3
C_Lag                              300            300            3
-------------------------------------------------------------------------------
No. of BFD Interfaces: 3
===============================================================================
*A:7210-SAS>show>router>bfd#

*A:7210-SAS>show>router>bfd# interface C_Lag

===============================================================================
BFD Interface
===============================================================================
Interface name                     Tx Interval    Rx Interval    Multiplier
-------------------------------------------------------------------------------
C_Lag                              300            300            3
-------------------------------------------------------------------------------
No. of BFD Interfaces: 1
===============================================================================
*A:7210-SAS>show>router>bfd#
```

neighbor

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

Context show>router

Description This command displays information about the IPv6 neighbor cache.

Parameters *ip-int-name* — Specify the IP interface name.

ip-address — Specify the address of the IPv6 interface address.

mac *ieee-mac-address* — Specify the MAC address.

summary — Displays summary neighbor information.

Output **Neighbor Output —** The following table describes neighbor output fields.

Label	Description
IPv6 Address	Displays the IPv6 address.
Interface	Displays the name of the IPv6 interface name.
MAC Address	Specifies the link-layer address.
State	Displays the current administrative state.
Exp	Displays the number of seconds until the entry expires.
Type	Displays the type of IPv6 interface.
Interface	Displays the interface name.
Rtr	Specifies whether a neighbor is a router.
Mtu	Displays the MTU size.

Sample Output

```
7210SAS# 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
===============================================================================
7210SAS#
```

session

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

Context show>router>bfd

Description This command displays session information.

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

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

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

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

Sample Output

```
*A:7210-SAS>show>router>bfd# session
===============================================================================
BFD Session
===============================================================================
Interface                      State                     Tx Intvl  Rx Intvl  Mult
  Remote Address               Protocol                  Tx Pkts   Rx Pkts
-------------------------------------------------------------------------------
F_Port                         Up (3)                    100       100       3
   22.1.1.1                    ospf2                     801259    801275
F_Lag                          Up (3)                    300       300       3
   23.1.1.1                    ospf2                     267087    267093
C_Lag                          Up (3)                    300       300       3
   25.1.1.2                    ospf2                     267005    266996
-------------------------------------------------------------------------------
No. of BFD sessions: 3
===============================================================================
*A:7210-SAS>show>router>bfd#
```

fib

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

Context show>router

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

Parameters *ip-prefix/prefix-length* — Displays FIB entries only matching the specified ip-prefix and length.

Values

ipv4-prefix:	a.b.c.d (host bits must be 0)
ipv4-prefix-length:	0 — 32

slot-number — Displays FIB entries only matching the specified slot number.

Values 1

longer — Displays FIB entries matching the *ip-prefix*/*mask* and routes with longer masks.

icmp6

Syntax **icmp6**

Context show>router

Description This command displays Internet Control Message Protocol Version 6 (ICMPv6) statistics. ICMP generates error messages (for example, ICMP destination unreachable messages) to report errors during processing and other diagnostic functions. ICMPv6 packets can be used in the neighbor discovery protocol and path MTU discovery.

Output **icmp6 Output —** The following table describes the show router icmp6 output fields:

Label	Description
`Total`	The total number of all messages.
`Destination Unreachable`	The number of message that did not reach the destination.
`Time Exceeded`	The number of messages that exceeded the time threshold.
`Echo Request`	The number of echo requests.
`Router Solicits`	The number of times the local router was solicited.
`Neighbor Solicits`	The number of times the neighbor router was solicited.
`Errors`	The number of error messages.
`Redirects`	The number of packet redirects.
`Pkt Too big`	The number of packets that exceed appropriate size.
`Echo Reply`	The number of echo replies.
`Router Advertise-ments`	The number of times the router advertised its location.
`Neighbor Adver-tisements`	The number of times the neighbor router advertised its location.

Sample Output

```
A:SR-3>show>router>auth# show router icmp6
===============================================================================
Global ICMPv6 Stats
===============================================================================
Received
Total                   : 14            Errors                  : 0
Destination Unreachable : 5             Redirects               : 5
Time Exceeded           : 0             Pkt Too Big             : 0
```

```
Echo Request           : 0            Echo Reply             : 0
Router Solicits        : 0            Router Advertisements  : 4
Neighbor Solicits      : 0            Neighbor Advertisements : 0
-------------------------------------------------------------------------------
Sent
Total                  : 10           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      : 5            Neighbor Advertisements : 5
===============================================================================
A:SR-3>show>router>auth#
```

interface

Syntax **interface** [*interface-name*]

Context show>router>icmpv6

Description This command displays interface ICMPv6 statistics.

Parameters *interface-name* — Only displays entries associated with the specified IP interface name.

Output **icmp6 interface Output —** The following table describes the show router icmp6 interface output fields:

Label	Description
Total	The total number of all messages.
Destination Unreachable	The number of message that did not reach the destination.
Time Exceeded	The number of messages that exceeded the time threshold.
Echo Request	The number of echo requests.
Router Solicits	The number of times the local router was solicited.
Neighbor Solicits	The number of times the neighbor router was solicited.
Errors	The number of error messages.
Redirects	The number of packet redirects.
Pkt Too big	The number of packets that exceed appropriate size.
Echo Reply	The number of echo replies.
Router Advertise-ments	The number of times the router advertised its location.
Neighbor Adver-tisements	The number of times the neighbor router advertised its location.

interface

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

Context show>router

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

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

Values

ip-int-name — Only displays the interface information associated with the specified IP interface name.

detail — Displays detailed IP interface information.

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

Label	Description
`Interface-Name`	The IP interface name.
`Type`	`n/a` — No IP address has been assigned to the IP interface, so the IP address type is not applicable. `Pri` — The IP address for the IP interface is the Primary address on the IP interface.
`IP-Address`	The IP address and subnet mask length of the IP interface. `n/a` — Indicates no IP address has been assigned to the IP interface.
`Adm`	`Down` — The IP interface is administratively disabled. `Up` — The IP interface is administratively enabled.
`Opr`	`Down` — The IP interface is operationally disabled. `Up` — The IP interface is operationally disabled.
`Mode`	`Network` — The IP interface is a network/core IP interface.
`Port`	The physical network port associated with the IP interface.

Sample Output

```
A:ALU-7210# show router interface
===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name                   Adm         Opr         Mode    Port/SapId
   IP-Address                                                    PfxState
-------------------------------------------------------------------------------
system                           Up          Up          Network system
   72.22.24.169/32                                               n/a
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
A:ALU-7210#
```

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

Label	Description
If Name	The IP interface name.
Admin State	Down — The IP interface is administratively disabled. Up — The IP interface is administratively enabled.
Oper State	Down — The IP interface is operationally disabled. Up — The IP interface is operationally enabled.
IP Addr/mask	The IP address and subnet mask length of the IP interface. Not Assigned — Indicates no IP address has been assigned to the IP interface.
If Index	The interface index of the IP router interface.
Virt If Index	The virtual interface index of the IP router interface.
Last Oper Change	The last change in operational status.
Global If Index	The global interface index of the IP router interface.
If Type	Network — The IP interface is a network/core IP interface.
SNTP B.cast	Displays if the broadcast-client global parameter is configured.
QoS Policy	The QoS policy ID associated with the IP interface.
MAC Address	The MAC address of the interface.
Arp Timeout	The ARP timeout for the interface, in seconds, which is the time an ARP entry is maintained in the ARP cache without being refreshed.
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 whether ARP is enabled or disabled.

Sample Output

```
A:SIM7# show router interface tosim6 detail
===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface
-------------------------------------------------------------------------------
If Name      : tosim6
Admin State  : Up                               Oper State       : Up
```

```
Protocols    : None
IP Addr/mask : 20.0.0.7/24                      Address Type     : Primary
IGP Inhibit  : Disabled                         Broadcast Address: Host-ones
-------------------------------------------------------------------------------
Details
-------------------------------------------------------------------------------
If Index     : 5                                Virt. If Index   : 5
Last Oper Chg: 01/09/2009 03:30:15              Global If Index  : 4
SAP Id       : 1/1/2:0.*
TOS Marking  : Untrusted                        If Type          : IES
SNTP B.Cast  : False                            IES ID           : 100
MAC Address  : 2e:59:01:01:00:02                Arp Timeout      : 14400
IP MTU       : 1500                             Arp Timeout      : 14400

ICMP Details
Redirects    : Number - 100                     Time (seconds)   - 10
Unreachables : Number - 100                     Time (seconds)   - 10
TTL Expired  : Number - 100                     Time (seconds)   - 10
===============================================================================
A:SIM7#

*A:ALU_SIM11>show>router>ldp# interface detail

===============================================================================
LDP Interfaces (Detail)
===============================================================================
-------------------------------------------------------------------------------
Interface "a"
-------------------------------------------------------------------------------
Admin State        : Up                 Oper State       : Up
Hold Time          : 15                 Hello Factor     : 3
Keepalive Timeout  : 30                 Keepalive Factor : 3
Transport Addr     : System             Last Modified    : 07/06/2010 10:36:59
Active Adjacencies : 1
Tunneling          : Disabled
Lsp Name           : None

===============================================================================
*A:ALU_SIM11>show>router>ldp#

*A:Dut-C# show router 1 mvpn
 ===============================================================================
MVPN 1 configuration data
===============================================================================
signaling          : Bgp                 auto-discovery     : Enabled
UMH Selection      : Highest-Ip          intersite-shared   : Enabled
vrf-import         : N/A
vrf-export         : N/A
vrf-target         : target:1:1
C-Mcast Import RT  : target:10.20.1.3:2

ipmsi              : pim-asm 224.1.1.1
admin status       : Up                  three-way-hello    : N/A
hello-interval     : N/A                 hello-multiplier   : 35 * 0.1
tracking support   : Disabled            Improved Assert    : N/A

spmsi              : pim-ssm 225.0.0.0/32
join-tlv-packing   : N/A
data-delay-interval: 3 seconds
```

```
data-threshold     : 224.0.0.0/4 --> 1 kbps
===============================================================================
```

policy

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

Context show>router

Description This command displays policy-related information.

Parameters *name* — Specify an existing policy-statement name.

prefix-list *name* **—** Specify a prefix list name to display the route policy entries.

admin — Specify the admin keyword to display the entities configured in the config>router>policy-options context.

route-table

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

Parameters *ip-prefix*[*/prefix-length*] **—** Displays routes only matching the specified ip-address and length.

Values ipv4-address: a.b.c.d (host bits must be set to 0)
ipv4-prefix-length: 0 — 32

longer — Displays routes matching the *ip-prefix*/*mask* and routes with longer masks.

exact — Displays the exact route matching the *ip-prefix*/*mask* masks.

summary — Displays a route table summary information.

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

Label	Description
`Dest Address`	The route destination address and mask.
`Next Hop`	The next hop IP address for the route destination.
`Type`	`Local` — The route is a local route.
	`Remote` — The route is a remote route.

Label	Description (Continued)
Protocol	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.

```
B:ALA-B# show router route-table 100.10.0.0 exact
===============================================================================
Route Table (Router: Base)
===============================================================================
Dest Address Next Hop Type Proto Age Metric Pref
-------------------------------------------------------------------------------
100.10.0.0/16 Black Hole Remote Static 00h03m17s 1 5
-------------------------------------------------------------------------------
No. of Routes: 1
===============================================================================
B:ALA-B#
```

Summary Route Table Output — Summary output for the route table displays the number of active routes and the number of routes learned by the router by protocol. Total active and available routes are also displayed.

Sample Output

```
A:ALA-A# show router route-table summary
===============================================================================
Route Table Summary
===============================================================================
                              Active                   Available
-------------------------------------------------------------------------------
Static                        1                        1
Direct                        6                        6
-------------------------------------------------------------------------------
Total
===============================================================================
A:ALA-A#
```

rtr-advertisement

Syntax **rtr-advertisement** [**interface** *interface-name*] [**prefix** *ipv6-prefix[/prefix-length]*]

Context show>router

Description This command displays router advertisement information.

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

Parameters *interface-name* — Maximum 32 characters.

ipv6-prefix[/*prefix-length*] — Displays routes only matching the specified ip-address and length.

Values	ipv6	ipv6-prefix[/pref*:	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 — FFFF]H d: [0 — 255]D
		prefix-length:	1 — 128

Output **Router-Advertisement Table Output —** The following table describes the output fields for router-advertisement.

Label	Description
`Rtr Advertisement Tx/Last Sent`	The number of router advertisements sent and time since they were sent.
`Nbr Solicitation Tx`	The number of neighbor solicitations sent and time since they were sent.
`Nbr Advertisement Tx`	The number of neighbor advertisements sent and time since they were sent.
`Rtr Advertisement Rx`	The number of router advertisements received and time since they were received.
`Nbr Advertisement Rx`	The number of neighbor advertisements received and time since they were received.
`Max Advert Inter-val`	The maximum interval between sending router advertisement mes-sages.
`Managed Config`	`True` — Indicates that DHCPv6 has been configured.
	`False` — Indicates that DHCPv6 is not available for address config-uration.
`Reachable Time`	The time, in milliseconds, that a node assumes a neighbor is reachable after receiving a reachability confirmation.
`Retransmit Time`	The time, in milliseconds, between retransmitted neighbor solicitation messages.
`Link MTU`	The MTU number the nodes use for sending packets on the link.
`Rtr Solicitation Rx`	The number of router solicitations received and time since they were received.
`Nbr Solicitation Rx`	The number of neighbor solicitations received and time since they were received.
`Min Advert Inter-val`	The minimum interval between sending ICMPv6 neighbor discovery router advertisement messages.
`Other Config`	`True` — Indicates there are other stateful configurations.

Label	Description (Continued)
	`False` — Indicates there are no other stateful configurations.
`Router Lifetime`	Displays the router lifetime in seconds.
`Hop Limit`	Displays the current hop limit.

Sample Output

```
A:7210SAS# show router rtr-advertisement
=======================================================================
Router Advertisement
=======================================================================
-------------------------------------------------------------------------------
Interface: interfaceNetworkNonDefault
-------------------------------------------------------------------------------
Rtr Advertisement Tx : 8                Last Sent            : 00h01m28s
Nbr Solicitation Tx  : 83               Last Sent            : 00h00m17s
Nbr Advertisement Tx : 74               Last Sent            : 00h00m25s
Rtr Advertisement Rx : 8                Rtr Solicitation Rx  : 0
Nbr Advertisement Rx : 83               Nbr Solicitation Rx  : 74
-------------------------------------------------------------------------------
Max Advert Interval  : 601              Min Advert Interval  : 201
Managed Config       : TRUE             Other Config         : TRUE
Reachable Time       : 00h00m00s400ms   Router Lifetime      : 00h30m01s
Retransmit Time      : 00h00m00s400ms   Hop Limit            : 63
Link MTU             : 1500

Prefix: 211::/120
Autonomous Flag      : FALSE            On-link flag         : FALSE
Preferred Lifetime   : 07d00h00m        Valid Lifetime       : 30d00h00m

Prefix: 231::/120
Autonomous Flag      : FALSE            On-link flag         : FALSE
Preferred Lifetime   : 49710d06h        Valid Lifetime       : 49710d06h

Prefix: 241::/120
Autonomous Flag      : TRUE             On-link flag         : TRUE
Preferred Lifetime   : 00h00m00s        Valid Lifetime       : 00h00m00s

Prefix: 251::/120
Autonomous Flag      : TRUE             On-link flag         : TRUE
Preferred Lifetime   : 07d00h00m        Valid Lifetime       : 30d00h00m
-------------------------------------------------------------------------------
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
-------------------------------------------------------------------------------
Interface: interfaceServiceNonDefault
-------------------------------------------------------------------------------
Rtr Advertisement Tx : 8                Last Sent            : 00h06m41s
Nbr Solicitation Tx  : 166              Last Sent            : 00h00m04s
Nbr Advertisement Tx : 143              Last Sent            : 00h00m05s
Rtr Advertisement Rx : 8                Rtr Solicitation Rx  : 0
```

```
Nbr Advertisement Rx : 166             Nbr Solicitation Rx  : 143
-------------------------------------------------------------------------------
Max Advert Interval  : 601             Min Advert Interval  : 201
Managed Config       : TRUE            Other Config         : TRUE
Reachable Time       : 00h00m00s400ms  Router Lifetime      : 00h30m01s
Retransmit Time      : 00h00m00s400ms  Hop Limit            : 63
Link MTU             : 1500

Prefix: 23::/120
Autonomous Flag      : FALSE           On-link flag         : FALSE
Preferred Lifetime   : infinite        Valid Lifetime       : infinite

Prefix: 24::/120
Autonomous Flag      : TRUE            On-link flag         : TRUE
Preferred Lifetime   : 00h00m00s       Valid Lifetime       : 00h00m00s

Prefix: 25::/120
Autonomous Flag      : TRUE            On-link flag         : TRUE
Preferred Lifetime   : 07d00h00m       Valid Lifetime       : 30d00h00m
-------------------------------------------------------------------------------
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

Prefix: 2::/120
Autonomous Flag      : TRUE            On-link flag         : TRUE
Preferred Lifetime   : 07d00h00m       Valid Lifetime       : 30d00h00m

Prefix: 23::/120
Autonomous Flag      : TRUE            On-link flag         : TRUE
Preferred Lifetime   : 07d00h00m       Valid Lifetime       : 30d00h00m

Prefix: 24::/119
Autonomous Flag      : TRUE            On-link flag         : TRUE
Preferred Lifetime   : 07d00h00m       Valid Lifetime       : 30d00h00m

Prefix: 25::/120
Autonomous Flag      : TRUE            On-link flag         : TRUE
Preferred Lifetime   : 07d00h00m       Valid Lifetime       : infinite

Prefix: 231::/120
Autonomous Flag      : TRUE            On-link flag         : TRUE
Preferred Lifetime   : 07d00h00m       Valid Lifetime       : 30d00h00m
-------------------------------------------------------------------------------
...
A:7210SAS#
```

static-arp

Syntax **static-arp** [*ip-addr* | *ip-int-name* | **mac** *ieee-mac-addr*]

Context show>router

Description This command displays the router static ARP table sorted by IP address. If no options are present, all ARP entries are displayed.

Parameters *ip-addr* — Only displays static ARP entries associated with the specified IP address.

ip-int-name — Only displays static ARP entries associated with the specified IP interface name.

mac *ieee-mac-addr* **—** Only displays static ARP entries associated with the specified MAC address.

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

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

Sample Output

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


A:ALA-A# show router static-arp 12.200.1.1
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Age      Type Interface
-------------------------------------------------------------------------------
```

```
12.200.1.1      00:00:5a:01:00:33 00:00:00 Inv  to-ser1

===============================================================================
A:ALA-A#


A:ALA-A# show router static-arp to-ser1
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Age      Type Interface
-------------------------------------------------------------------------------
10.200.0.253  00:00:5a:40:00:01 00:00:00 Sta to-ser1
===============================================================================
A:ALA-A#


A:ALA-A# show router static-arp mac 00:00:5a:40:00:01
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Age      Type Interface
-------------------------------------------------------------------------------
10.200.0.253  00:00:5a:40:00:01 00:00:00 Sta to-ser1
===============================================================================
A:ALA-A#
```

static-route

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

Context show>router

Description This command displays the static entries in the routing table. If no options are present, all static routes are displayed sorted by prefix.

Parameters *ip-prefix* /*mask* — Displays static routes only matching the specified *ip-prefix* and *mask*.

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

detail — Displays detail information.

preference *preference* — Only displays static routes with the specified route preference.

Values 0 — 65535

next-hop *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)

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

Label	Description
IP Addr/mask	The static route destination address and mask.

Label	Description (Continued)
`Pref`	The route preference value for the static route.
`Metric`	The route metric value for the static route.
`Type`	`BH` — The static route is a black hole route. The `Nexthop` for this type of route is `black-hole`. `ID` — The static route is an indirect route, where the `nexthop` for this type of route is the non-directly connected next hop. `NH` — The route is a static route with a directly connected next hop. The `Nexthop` for this type of route is either the next hop IP address or an egress IP interface name.
`Next Hop`	The next hop for the static route destination.
`Protocol`	The protocol through which the route was learned.
`Interface`	The egress IP interface name for the static route. `n/a` — indicates there is no current egress interface because the static route is inactive or a black hole route.
`Active`	`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.
`No. of Routes`	The number of routes displayed in the list.

Sample Output

```
A:ALA-A# show router static-route
===============================================================================
Route Table
===============================================================================
IP Addr/mask       Pref Metric Type Nexthop              Interface       Active
-------------------------------------------------------------------------------
192.168.250.0/24   5    1      ID   10.200.10.1          to-ser1              Y
192.168.252.0/24   5    1      NH   10.10.0.254          n/a                  N
192.168.253.0/24   5    1      NH   to-ser1              n/a                  N
192.168.253.0/24   5    1      NH   10.10.0.254          n/a                  N
192.168.254.0/24   4    1      BH   black-hole           n/a                  Y
===============================================================================
A:ALA-A#


A:ALA-A# show router static-route 192.168.250.0/24
===============================================================================
Route Table
===============================================================================
IP Addr/mask       Pref Metric Type Nexthop              Interface       Active
-------------------------------------------------------------------------------
192.168.250.0/24   5    1      ID   10.200.10.1          to-ser1              Y
===============================================================================
```

```
A:ALA-A#

A:ALA-A# show router static-route preference 4
===============================================================================
Route Table
===============================================================================
IP Addr/mask       Pref Metric Type Nexthop             Interface       Active
-------------------------------------------------------------------------------
192.168.254.0/24   4    1      BH   black-hole          n/a                  Y
===============================================================================
A:ALA-A#

A:ALA-A# show router static-route next-hop 10.10.0.254
===============================================================================
Route Table
===============================================================================
IP Addr/mask       Pref Metric Type Nexthop             Interface       Active
-------------------------------------------------------------------------------
192.168.253.0/24   5    1      NH   10.10.0.254         n/a                  N
===============================================================================
A:ALA-A#
```

status

Syntax **status**

Context show>router

Description This command displays the router status.

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

Label	Description
Router	The administrative and operational states for the router.
OSPF	The administrative and operational states for the OSPF protocol.
ISIS	The administrative and operational states for the IS-IS protocol.
MPLS	The administrative and operational states for the MPLS protocol.
LDP	The administrative and operational states for the LDP protocol.
BGP	The administrative and operational states for the BGP protocol.
Max Routes	The maximum number of routes configured for the system.
Total Routes	The total number of routes in the route table.
ECMP Max Routes	The number of ECMP routes configured for path sharing.

Label	Description (Continued)
Triggered Policies	No — Triggered route policy re-evaluation is disabled. Yes — Triggered route policy re-evaluation is enabled.

Sample Output

Note that there are multiple instances of OSPF. OSPF-0 is persistent. OSPF-1 through OSPF-31 are present when that particular OSPF instance is configured.

```
*A:7210-SAS>show>router# status

===============================================================================
Router Status (Router: Base)
===============================================================================
                         Admin State                        Oper State
-------------------------------------------------------------------------------
Router                   Up                                 Up
OSPFv2-0                 Up                                 Up
ISIS                     Not configured                     Not configured
MPLS                     Up                                 Up
RSVP                     Up                                 Up
LDP                      Not configured                     Not configured
BGP                      Up                                 Up
OSPFv3                   Not configured                     Not configured

Max IPv4 Routes          16000
Max IPv6 Routes          No Limit
Total IPv4 Routes        3
Total IPv6 Routes        0
ECMP Max Routes          1
Mcast Info Policy        default
Triggered Policies       No
===============================================================================
*A:7210-SAS>show>router#
```

tunnel-table

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

Context show>router

Description This command displays tunnel table information. Note that auto-bind GRE tunnels are not displayed in **show** command output. GRE tunnels are not the same as SDP tunnels that use the GRE encapsulation type.

Parameters *ip-address*[/*mask*] — Displays the specified tunnel table's destination IP address and mask.

protocol *protocol* — Dislays LDP protocol information.

sdp *sdp-id* — Displays information pertaining to the specified SDP.

summary — Displays summary tunnel table information.

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

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

Sample Output

```
A:ALA-A>config>service# show router tunnel-table
===============================================================================
Tunnel Table
===============================================================================
Destination Owner  Encap    Tunnel Id    Pref   Nexthop    Metric
-------------------------------------------------------------------------------
10.0.0.1/32  sdp     GRE        10        5    10.0.0.1      0
10.0.0.1/32  sdp     GRE        21        5     10.0.0.1     0
10.0.0.1/32  sdp     GRE        31        5     10.0.0.1     0
10.0.0.1/32  sdp     GRE        41        5     10.0.0.1     0
===============================================================================
A:ALA-A>config>service#
```

```
A:ALA-A>config>service#  show router tunnel-table summary
===============================================================================
Tunnel Table Summary (Router: Base)
===============================================================================
                              Active                   Available
-------------------------------------------------------------------------------
LDP                           1                        1
SDP                           1                        1
===============================================================================
A:ALA-A>config>service#
```

Clear Commands

router

Syntax **router**

Context clear>router

Description This command clears for a the router instance in which they are entered.

Parameters *router-instance* — Specify the router name or service ID.

Values Base, management

Default Base

arp

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

Context clear>router

Description This command clears all or specific ARP entries.

The scope of ARP cache entries cleared depends on the command line option(s) specified.

Parameters **all —** Clears all ARP cache entries.

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

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

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

icmp6

Syntax **icmp6 all**
icmp6 global
icmp6 interface *interface-name*

Context clear>router

Description This command clears ICMP statistics.

Parameters **all —** Clears all statistics.

global — Clears global statistics.

interface-name — Clears ICMP6 statistics for the specified interface.

bfd

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

Context clear>router

Description This command enables the context to clear bi-directional forwarding (BFD) sessions and statistics.

session

Syntax **session src-ip** *ip-address* **dst-ip** *ip-address*

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 remote endpoint of this BFD session.

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.

neighbor

Syntax **neighbor** {**all** | *ip-address [***interface** *interface-name}*
neighbor [**interface** *ip-int-name* | *ipv6-address*]

Context clear>router

Description This command clears IPv6 neighbor information.

Parameters **all —** Clears IPv6 neighbors.

ip-int-name — Clears the specified neighbor interface information.

Values 32 characters maximum

ip-address — Clears the specified IPv6 neighbors.

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 — FFFF]H
d: [0 — 255]D

router-advertisement

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

Context clear>router

Description This command clears all router advertisement counters.

Parameters *all* — Clears all router advertisement counters for all interfaces.

interface *interface-name* **—** Clear router advertisement counters for the specified interface.

Debug Commands

router

Syntax **router**

Context debug

Description This command configures debugging for a router instance.

Parameters *router-instance* — Specify the router name or service ID.

Values *router-name*: Base
service-id: 1 — 2147483647

Default Base

ip

Syntax **ip**

Context debug>router

Description This command configures debugging for IP.

arp

Syntax **arp**

Context debug>router>ip

Description This command configures route table debugging.

icmp

Syntax [**no**] **icmp**

Context **debug>router>ip**

Description This command enables ICMP debugging.

icmp6

Syntax **icmp6** [*ip-int-name*]
no icmp6

Context debug>router>ip

Description This command enables ICMP6 debugging.

interface

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

Context debug>router>ip

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

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

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

ip-int-name — Only displays the interface information associated with the specified IP interface name.

Values 32 characters maximum

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 debugging for IP packets.

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

Values 32 characters maximum

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

Values ipv4-address a.b.c.d (host bits must be 0)
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 — FFFF]H
d: [0 — 255]D

headers — Only displays information associated with the packet header.

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

Values 0 — 255 (values can be expressed in decimal, hexidecimal, or binary)
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, 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*]
route-table *ip-prefix*/*prefix-length* **longer**
no route-table

Context debug>router>ip

Description This command configures route table debugging.

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

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

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

VRRP

In This Chapter

This chapter provides information about configuring Virtual Router Redundancy Protocol (VRRP) parameters. Topics in this chapter include:

VRRP Overview

NOTE: VRRP for IPv4 is supported only in 7210 SAS-M network mode and 7210 SAS-X. It is not supported in 7210 SAS-M access-uplink mode. VRRP for IPv6 is not supported on 7210 platforms.

The Virtual Router Redundancy Protocol (VRRP) for IPv4 is defined in the IETF RFC 3768, *Virtual Router Redundancy Protocol*. VRRP describes 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. When this IP interface is specified as a default gateway on hosts directly attached to this LAN, the routers sharing the IP interface prevent a single point of failure by limiting access to this gateway address. VRRP can be implemented on IES service interfaces, VPRN interfaces, and on core network IP interfaces.

If the master virtual router fails, the backup router configured with the highest acceptable priority becomes the master virtual router. The new master router assumes the normal packet forwarding for the local hosts.

Figure 3 displays an example of a VRRP configuration.

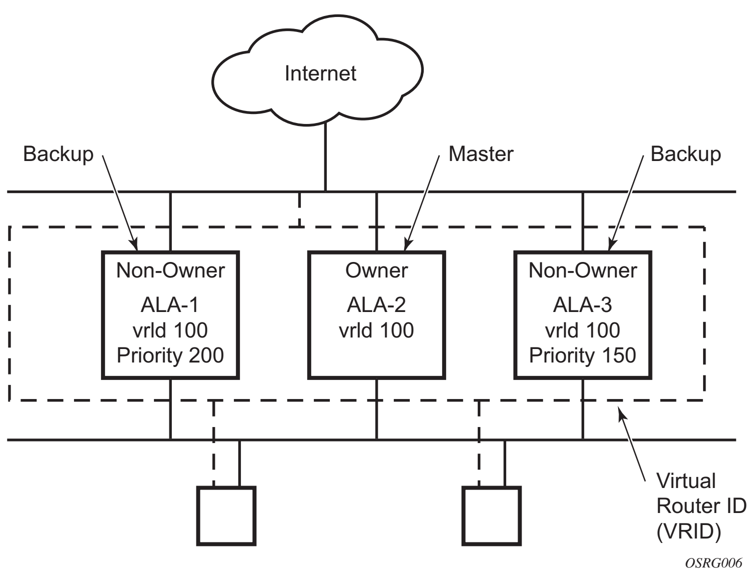


Figure 3: VRRP Configuration

VRRP Components

VRRP consists of the following components:

- Virtual Router on page 119
- IP Address Owner on page 119
- Primary IP Addresses on page 120
- Virtual Router Master on page 120
- Virtual Router Backup on page 121
- Owner and Non-Owner VRRP on page 121

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 Identifier (VRID) and a set of associated IP addresses (or address) across a common LAN. A VRRP router can backup one or more virtual routers.

Up to four virtual routers are possible on a single Alcatel-Lucent IP interface. The virtual routers must be in the same subnet. Each virtual router has its own VRID, state machine and messaging instance.

IP Address Owner

VRRP can be configured in either an owner or non-owner mode. The owner is the VRRP router whose virtual router IP address is the same as the real interface IP address. This is the router that responds to packets addressed to one of the IP addresses for ICMP pings, TCP connections, and others. All other virtual router instances participating in this message domain must have the same VRID configured and cannot be configured as owner.

7210 SASallows the virtual routers to be configured as non-owners of the IP address. VRRP on a router can be configured to allow non-owners to respond to ICMP echo requests when they become the virtual router master for the virtual router. Telnet and other connection-oriented protocols can also be configured for non-owner master response. However, the individual application conversations (connections) will not survive a VRRP failover. A non-owner VRRP router operating as a backup will not respond to any packets addressed to any of the virtual router IP addresses.

Primary IP Addresses

A primary address is an IP address selected from the set of real interface address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.

A IP interface must always have a primary IP address assigned for VRRP to be active on the interface. VRRP supports only primary addresses. The virtual router's VRID primary IP address is always the primary address on the IP interface. VRRP uses the primary IP address as the IP address placed in the source IP address field of the IP header for all VRRP messages sent on that interface.

Virtual Router Master

The VRRP router which controls the IP address(es) associated with a virtual router is called the master. The master is responsible for forwarding packets sent to the VRRP IP addresses. An election process provides dynamic failover of the forwarding responsibility 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. This 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 backup virtual router for the VRID compare the configured priority values to determine the master role. In case of a tie, the virtual router with the highest primary IP address becomes master.

The `preempt` parameter can be set to `false` to prevent a backup virtual router with a better priority value from becoming master when an existing non-owner virtual router is the current master. This is determined on a first-come, first-served basis.

While 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.

Virtual Router Backup

A new virtual router master is selected from the set of VRRP routers available to assume forwarding responsibility for a virtual router should the current master fail.

Owner and Non-Owner VRRP

The owner controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. The owner assumes the role of the master virtual router. Only one virtual router in the domain can be configured as owner. All other virtual router instances participating in this message domain must have the same VRID configured.

The most important parameter to be defined on a non-owner virtual router instance is the priority. The priority defines a virtual router's selection order in the master election process. The priority value and the preempt mode determine the virtual router with the highest priority to become the master virtual router.

The base priority is used to derive the in-use priority of the virtual router instance as modified by any optional VRRP priority control policy. VRRP priority control policies can be used to either override or adjust the base priority value depending on events or conditions within the chassis.

For information about non-owner access parameters, refer to VRRP Non-Owner Accessibility on page 136.

Configurable Parameters

In addition to backup IP addresses, to facilitate configuration of a virtual router on routers, the following parameters can be defined in owner configurations:

- Virtual Router ID (VRID) on page 122
- Message Interval and Master Inheritance on page 124
- VRRP Message Authentication on page 126
- Authentication Data on page 128
- Virtual MAC Address on page 128

The following parameters can be defined in non-owner configurations:

- Virtual Router ID (VRID) on page 122
- Priority on page 122
- Message Interval and Master Inheritance on page 124
- Master Down Interval on page 125
- Preempt Mode on page 125
- VRRP Message Authentication on page 126
- Authentication Data on page 128
- Virtual MAC Address on page 128
- Policies on page 129

Virtual Router ID (VRID)

The VRID must be configured with the same value on each virtual router associated with the redundant IP address (IP addresses). It is placed in all VRRP advertisement messages sent by each virtual router.

Priority

The priority value affects the interaction between this VRID and the same VRID of other virtual routers participating on the same LAN. A higher priority value defines a greater priority in becoming the virtual router master for the VRID. The priority value can only be configured when the defined IP address on the IP interface is different than the virtual router IP address (non-owner mode).

When 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.

The priority value 0 is reserved for VRRP advertisement message purposes. It is used to tell other virtual routers in the same VRID that this virtual router is no longer acting as master, triggering a new election process. When this happens, each backup virtual router sets its master down timer equal to the skew time value. This shortens the time until one of the backup virtual routers becomes master.

The current master virtual router must transmit a VRRP advertisement message immeediately upon receipt of a VRRP message with priority set to 0. This prevents another backup from becoming master for a short period of time.

Non-owner virtual routers may be configured with a priority of 254 through 1. The default value is 100. Multiple non-owners can share the same priority value. When multiple non-owner backup virtual routers are tied (transmit VRRP advertisement messages simultaneously) in the election process, both become master simultaneously, the one with the best priority will win the election. If the priority value in the message is equal to the master's local priority value, then the primary IP address of the local master and the message is evaluated as the tie breaker. The higher IP address becomes master. (The primary IP address is the source IP address of the VRRP advertisement message.)

The priority is also used to determine when to preempt the existing master. If the preempt mode value is true, VRRP advertisement messages from inferior (lower priority) masters are discarded, causing the master down timer to expire and the transition to master state.

The priority value also dictates the skew time added to the master timeout period.

IP Addresses

Each virtual router participating in the same VRID should be defined with the same set of IP addresses. These are the IP addresses being used by hosts on the LAN as gateway addresses.

Message Interval and Master Inheritance

Each virtual router is configured with a message interval per VRID within which it participates. This parameter must be the same for every virtual router on the VRID.

For IPv4, the default advertisement interval is 1 second and can be configured between 1 second and 255 seconds and 900 milliseconds.

NOTE: 7210 SAS supports a minimum message interval of 1 second. It does not support use of sub-second message intervals.

As specified in the RFC, the advertisement interval field in every received VRRP advertisement message must match the locally configured advertisement interval. If a mismatch occurs, depending on the inherit configuration, the current master's advertisement interval setting can be used to operationally override the locally configured advertisement interval setting. If the current master changes, the new master setting is used. If the local virtual router becomes master, the locally configured advertisement interval is enforced.

If a VRRP advertisement message is received with an advertisement interval set to a value different than the local value and the inherit parameter is disabled, the message is discarded without processing.

The master virtual router on a VRID uses the advertisement interval to load the advertisement timer, specifying when to send the next VRRP advertisement message. Each backup virtual router on a VRID uses the advertisement interval (with the configured local priority) to derive the master down timer value.

VRRP advertisements messages that are fragmented contain IP options (IPv4) require a longer message interval to be configured.

Skew Time

The skew time is used to add a time period to the master down interval. This is not a configurable parameter. It is derived from the current local priority of the virtual router’s VRID. To calculate the skew time, the virtual router evaluates the following formula:

For IPv4: Skew Time = ((256 - priority) / 256) seconds

The higher priority value, the smaller the skew time will be. This means that virtual routers with a lower priority will transition to master slower than virtual routers with higher priorities.

Master Down Interval

The master down interval is a calculated value used to load the master down timer. When the master down timer expires, the virtual router enters the master state. To calculate the master down interval, the virtual router evaluates the following formula:

Master Down Interval = (3 x Operational Advertisement Interval) + Skew Time

The operational advertisement interval is dependent upon the state of the inherit parameter. When the inherit parameter is enabled, the operational advertisement interval is derived from the current master's advertisement interval field in the VRRP advertisement message. When inherit is disabled, the operational advertisement interval must be equal to the locally configured advertisement interval.

The master down timer is only operational when the local virtual router is operating in backup mode.

Preempt Mode

Preempt mode is a true or false configured value which controls whether a specific backup virtual router preempts a lower priority master. The IP address owner will always become master when available. Preempt mode cannot be set to false on the owner virtual router. The default value for preempt mode is true.

When preempt mode is true, the advertised priority from the incoming VRRP advertisement message from the current master is compared to the local configured priority. If the local priority is higher, the received VRRP advertisement message is discarded. This will result in the eventual expiration of the master down timer causing a transition to the master state. If the received priority is equal to the local priority, the message is not discarded and the current master will not be discarded. Note that when in the backup state, the received primary IP address is not part of the decision to preempt and is not used as a tie breaker when the received and local priorities are equal.

When `preempt` is enabled, the virtual router instance overrides any non-owner master with an in-use message priority value less than the virtual router instance in-use priority value. If `preempt` is disabled, the virtual router only becomes master if the master down timer expires before a VRRP advertisement message is received from another virtual router.

VRRP Message Authentication

The authentication type parameter defines the type of authentication used by the virtual router in VRRP advertisement message authentication. VRRP message authentication is applicable to IPv4 only. The current master uses the configured authentication type to indicate any egress message manipulation that must be performed in conjunction with any supporting authentication parameters before transmitting a VRRP advertisement message. The configured authentication type value is transmitted in the message authentication type field with the appropriate authentication data field filled in. Backup routers use the authentication type message field value in interpreting the contained authentication data field within received VRRP advertisement messages.

VRRP supports three message authentication methods which provide varying degrees of security. The supported authentication types are:

0 – No Authentication

1 – Simple Text Password

Authentication Type 0 – No Authentication

The use of type 0 indicates that VRRP advertisement messages are not authenticated (provides no authentication). The master transmitting VRRP advertisement messages will transmit the value 0 in the egress messages authentication type field and the authentication data field. Backup virtual routers receiving VRRP advertisement messages with the authentication type field equal to 0 will ignore the authentication data field in the message.

All compliant VRRP advertisement messages are accepted. The following fields within the received VRRP advertisement message are checked for compliance (the VRRP specification may require additional checks).

- IP header checks specific to VRRP
  - → IP header destination IP address – Must be 224.0.0.18
  - → IP header TTL field – Must be equal to 255, the packet must not have traversed any IP routed hops
  - → IP header protocol field – must be 112 (decimal)

- VRRP message checks
  - → Version field – Must be set to the value 2
  - → Type field – Must be set to the value of 1 (advertisement)
  - → Virtual router ID field – Must match one of the configured VRID on the ingress IP interface (All other fields are dependent on matching the virtual router ID field to one of the interfaces configured VRID parameters)
  - → Priority field – Must be equal to or greater than the VRID in-use priority or be equal to 0 (Note, equal to the VRID in-use priority and 0 requires further processing regarding master/backup and senders IP address to determine validity of the message)
  - → Authentication type field – Must be equal to 0
  - → Advertisement interval field – Must be equal to the VRID configured advertisement interval
  - → Checksum field – Must be valid
  - → Authentication data fields – Must be ignored.

VRRP messages not meeting the criteria are silently dropped.

Authentication Type 1 – Simple Text Password

The use of type 1 indicates that VRRP advertisement messages are authenticated with a clear (simple) text password. All virtual routers participating in the virtual router instance must be configured with the same 8 octet password. Transmitting virtual routers place a value of 1 in the VRRP advertisement message authentication type field and put the configured simple text password into the message authentication data field. Receiving virtual routers compare the message authentication data field with the local configured simple text password based on the message authentication type field value of 1.

The same checks are performed for type 0 with the following exceptions (the VRRP specification may require additional checks):

- VRRP message checks
  - → Authentication type field – Must be equal to 1
  - → Authentication data fields – Must be equal to the VRID configured simple text password

Any VRRP message not meeting the type 0 verification checks with the exceptions above are silently discarded.

Authentication Failure

Any received VRRP advertisement message that fails authentication must be silently discarded with an invalid authentication counter incremented for the ingress virtual router instance.

Authentication Data

This feature is different than the VRRP advertisement message field with the same name. This is any required authentication information that is pertinent to the configured authentication type. The type of authentication data used for each authentication type is as follows:

Authentication Type	Authentication Data
0	None, authentication is not performed
1	Simple text password consisting of 8 octets

Virtual MAC Address

On 7210 SAS, the MAC address is not configurable. 7210 SAS derives the MAC address to use from the VRID assigned as defined in the standard.

VRRP Advertisement Message IP Address List Verification

VRRP advertisement 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 implementation always logs mismatching events. The decision on where and whether to forward the generated messages depends on the configuration of the event manager.

To facilitate the sending of mismatch log messages, each virtual router instance keeps the mismatch state associated with each source IP address in the VRRP master table. Whenever 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.

Owner and non-owner virtual router instances have the supported IP addresses explicitly defined, making mismatched supported IP address within the interconnected virtual router instances a provisioning issue.

Policies

Policies can be configured to control VRRP priority with the virtual router instance. VRRP priority control policies can be used to override or adjust the base priority value depending on events or conditions within the chassis.

The policy can be associated with more than one virtual router instance. The priority events within the policy override or diminish the base priority dynamically affecting the in-use priority. As priority events clear in the policy, the in-use priority can eventually be restored to the base priority value.

Policies can only be configured in the non-owner VRRP context. For non-owner virtual router instances, if policies are not configured, then the base priority is used as the in-use priority.

VRRP Priority Control Policies

This implementation of VRRP supports control policies to manipulate virtual router participation in the VRRP master election process and master self-deprecation. The local priority value for the virtual router instance is used to control the election process and master state.

VRRP Virtual Router 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 are required to have a priority value of 255 that cannot be diminished. Only one VRRP priority control policy can be applied to a non-owner virtual router instance.

Multiple VRRP virtual router instances may 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 when the preempt mode has been enabled. A virtual router instance with preempt mode disabled will always use the base priority as the in-use priority, ignoring any configured priority control policy.

VRRP Virtual Router Instance Base Priority

Non-owner virtual router instances must have a base priority value between 1 and 254. The value 0 is reserved for master termination. The value 255 is reserved for owners. The default base priority for non-owner virtual router instances is the value 100.

The base priority is the starting priority for the VRRP instance. The actual in-use priority for the VRRP instance is derived from the base priority and an optional VRRP priority control policy.

VRRP Priority Control Policy Delta In-Use Priority Limit

A VRRP priority control policy enforces an overall minimum value that the policy can inflict on the VRRP virtual router instance base priority. This value provides a lower limit to the delta priority events 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, in-use 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, less the sum of the delta values derives the actual priority value in-use.

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. When 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.

VRRP Priority Control Policy Priority Events

The main function of a VRRP priority control policy is to define conditions or events that impact the system's ability to communicate with outside hosts or portions of the network. When one or multiple 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 may be configured as an explicit event or a delta event.

Explicit events override all delta events. When 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 reevaluated accordingly and adjusted dynamically.

Delta priority events also have priority values. When 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 when the event is no longer true, indicating that it has been cleared.

Priority Event Hold-Set Timers

Hold-set timers are used to dampen the effect of a flapping event. A flapping event is where the event continually transitions between clear and set. The hold-set value is loaded into a hold set timer that prevents a set event from transitioning to the cleared state until it expires.

Each time an event transitions between cleared and set, the timer is loaded and begins to count down to zero. If the timer reaches zero, the event will be 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 a further set action reload the hold set timer. This extends the amount of time that must expire before entering the cleared state.

For an example of a hold-set timer setting, refer to LAG Degrade Priority Event on page 133.

Port Down Priority Event

The port down priority event is tied to either a physical port or a SONET/SDH channel. The port or channel operational state is evaluated to determine a port down priority event or event clear.

When the port or channel operational state is up, the port down priority event is considered false or cleared. When the port or channel operational state is down, the port down priority event is considered true or set.

LAG Degrade Priority Event

The LAG degrade priority event is tied to an existing Link Aggregation Group (LAG). The LAG degrade priority event is conditional to percentage of available port bandwidth on the LAG. Multiple bandwidth percentage thresholds may be defined, each with its own priority value.

If the LAG transitions from one threshold to the next, the previous threshold priority value is subtracted from the total delta sum while the new threshold priority value is added to the sum. The new sum is then subtracted from the base priority and compared to the delta in-use priority limit to derive the new in-use priority on the virtual router instance.

The following example illustrates a LAG priority event and it’s interaction with the hold set timer in changing the in-use priority.

The following state and timer settings are used for the LAG events displayed in Table 5:

- User-defined thresholds: 2 ports down 3 ports down
- LAG configured ports: 4 ports
- Hold set timer (hold-set): 5 seconds

Table 5: LAG Events

Time	LAG Port State	Parameter	State	Comments
0	All ports down	Event State	Set - 4 ports down	
		Event Threshold	3 ports down	
		Hold Set Timer	5 seconds	Set to **hold-set** parameter

Table 5: LAG Events (Continued)

Time	LAG Port State	Parameter	State	Comments
1	One port up	Event State	Set - 4 ports down	Cannot change until Hold Set Timer expires
		Event Threshold	3 ports down	
		Hold Set Timer	5 seconds	Event does not affect timer
2	All ports up	Event State	Set - 4 ports down	Still waiting for Hold Set Timer expires
		Event Threshold	3 ports down	
		Hold Set Timer	3 seconds	
5	All ports up	Event State	Cleared - All ports up	
		Event Threshold	None	Event cleared
		Hold Set Timer	Expired	
100	Three ports down	Event State	Set - 3 ports down	
		Event Threshold	3 ports down	
		Hold Set Timer	Expired	Set to **hold-set** parameter
102	Two ports down	Event State	Set - 3 ports down	
		Event Threshold	3 ports down	
		Hold Set Timer	3 seconds	
103	All ports up	Event State	Set - 3 ports down	
		Event Threshold	3 ports down	
		Hold Set Timer	2 second	
104	One ports down	Event State	Set - 3 ports down	
		Event Threshold	3 ports down	
		Hold Set Timer	1 second	Current threshold is 2, so 1 down has no effect
105	One ports down	Event State	Set - 1 port down	
		Event Threshold	2 ports down	
		Hold Set Timer	Expired	

Host Unreachable Priority Event

The host unreachable priority event creates a continuous ping task that is used to test connectivity to a remote host. The path to the remote host and the remote host itself must be capable and configured to accept ICMP echo request and replies for the ping to be successful.

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 when the ping destination is considered unreachable.

When the host is unreachable, the host unreachable priority event is considered true or set. When the host is reachable, the host unreachable priority event is considered false or cleared.

Route Unknown Priority Event

The route unknown priority event defines a task that monitors the existence of a given route prefix in the system's routing table.

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.

When 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. When a route prefix does not exist within the active route table matching the defined criteria, the route unknown priority event is considered true or set.

VRRP Non-Owner Accessibility

Although the RFC states that only VRRP owners can respond to ping and other management-oriented protocols directed to the VRID IP addresses, allows an override of this restraint on a per VRRP virtual router instance basis.

Non-Owner Access Ping Reply

When non-owner access ping reply is enabled on a virtual router instance, ICMP echo request messages destined to the non-owner virtual router instance IP addresses are not discarded at the IP interface when operating in master mode. ICMP echo request messages are always discarded in backup mode.

When non-owner access ping reply is disabled on a virtual router instance, ICMP echo request messages destined to the non-owner virtual router instance IP addresses are silently discarded in both the master and backup modes.

Non-Owner Access Telnet

When non-owner access Telnet is enabled on a virtual router instance, authorized Telnet sessions may be established that are destined to the virtual router instance IP addresses when operating in master mode. Telnet sessions are always discarded at the IP interface when destined to a virtual router IP address 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.

When non-owner access Telnet is disabled on a virtual router instance, Telnet sessions destined to the non-owner virtual router instance IP addresses are silently discarded in both master and backup modes.

Non-Owner Access SSH

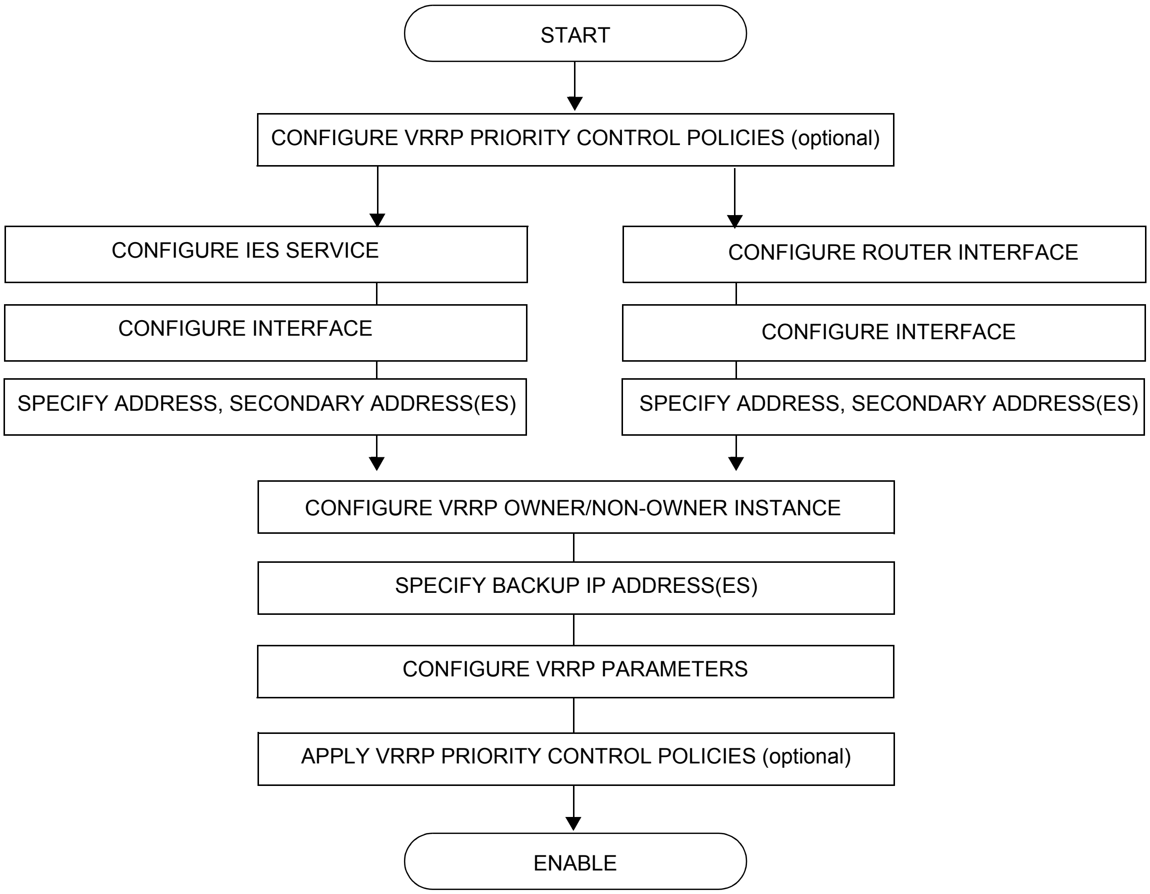
When non-owner access SSH is enabled on a virtual router instance, authorized SSH sessions may be established that are destined to the virtual router instance IP addresses when operating in master mode. SSH sessions are always discarded at the IP interface when destined to a virtual router IP address 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.

When non-owner access SSH is disabled on a virtual router instance, SSH sessions destined to the non-owner virtual router instance IP addresses are silently discarded in both master and backup modes.

VRRP Configuration Process Overview

Figure 4 displays the process to provision VRRP parameters.

Figure 4: VRRP Configuration and Implementation Flow



Configuration Notes

This section describes VRRP configuration caveats.

General

- Creating and applying VRRP policies are optional.
- Backup command:
  - → The backup IP address(es) must be on the same subnet. The backup addresses explicitly define which IP addresses are in the VRRP advertisement message IP address list.
  - → In the owner mode, the backup IP address must be identical to one of the interface's IP addresses. The backup address explicitly defines which IP addresses are in the VRRP advertisement message IP address list.

Configuring VRRP with CLI

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

Topics in this section include:

VRRP Configuration Overview

Configuring VRRP policies and configuring VRRP instances on interfaces and router interfaces is optional. The basic owner and non-owner VRRP configurations on an IES or router 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 address shared between two or more routers connecting the common domain. VRRP provides dynamic fail over of the forwarding responsibility 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.

Preconfiguration Requirements

VRRP policies:

- VRRP policies must be configured before they can be applied to an interface or IES VRRP instance. VRRP policies are configured in the **config>vrrp** context.

Configuring VRRP on an IES service interface:

- The service customer account must be created prior to configuring an IES VRRP instance.
- The interface address must be specified in the both the owner and non-owner IES or router interface instances.

Basic VRRP Configurations

Configure VRRP parameters in the following contexts:

- VRRP Policy on page 143
- VRRP IES Service Parameters on page 144
- VRRP Router Interface Parameters on page 145

VRRP Policy

Configuring and applying VRRP policies are optional. There are no default VRRP policies. Each policy must be explicitly defined. A VRRP configuration must include the following:

- Policy ID
- Define at least one of the following priority events:
  → Port down
  → LAG port down
  → Host unreachable
  → Route unknown

The following example displays a sample configuration of a VRRP policy.

```
A:SR2>config>vrrp>policy# info
----------------------------------------------
            delta-in-use-limit 50
            priority-event
                port-down /1/2
                    hold-set 43200
                    priority 100 delta
                exit
                port-down /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
                exit
            exit
----------------------------------------------
```

VRRP IES Service Parameters

VRRP parameters are configured within an IES service with two contexts, owner or non-owner. The status is specified when the VRRP configuration is created. When configured as owner, the virtual router instance owns the 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.

For IPv4, up to 4 virtual routers IDs (vrid) can be configured on an IES service interface.

VRRP parameters configured within an IES service must include the following:

- VRID
- Backup IP address(es)

The following example displays a sample configuration of a IES service owner and non-owner VRRP configurations.

```
A:SR2>config>service>ies# info
----------------------------------------------
            interface "tuesday" create
                address 10.10.36.2/24
                sap 7/1/1.2.2 create
                vrrp 19 owner
                    backup 10.10.36.2
                    authentication-type password
                    authentication-key "testabc"
                exit
            exit
            interface "testing" create
                address 10.10.10.16/24
                sap 1/1/55:0 create
                vrrp 12
                    backup 10.10.10.15
                    policy 1
                    authentication-type password
                    authentication-key "testabc"
                exit
            exit
            no shutdown
----------------------------------------------
A:SR2>config>service>ies#
```

VRRP Router Interface Parameters

VRRP parameters are configured on a router interface with two contexts, owner or non-owner. The status is specified when the VRRP configuration is created. When configured as owner, the virtual router instance owns the backed up IP addresses. All other virtual router instances participating in this message domain must have the same `vrid` configured and cannot be configured as owner.

For IPv4, up to 4 virtual routers IDs (vrid) can be configured on a router interface.

VRRP parameters configured on a router interface must include the following:

- VRID
- Backup IP address(es)

The following example displays a sample configuration of a router interface owner and non-owner VRRP configurations.

```
A:SR4>config>router# info
#------------------------------------------
echo "IP Configuration "
#------------------------------------------
        interface "system"
            address 10.10.0.4/32
        exit
        interface "test1"
            address 10.10.14.1/24
                    exit
        interface "test2"
            address 10.10.10.23/24
            vrrp 1 owner
                backup 10.10.10.23
                              authentication-key "testabc"
            exit
        exit
#------------------------------------------
A:SR4>config>router#
```

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure VRRP and provides the CLI commands.

VRRP parameters are defined under a service interface or a router interface context. An IP address must be assigned to each IP interface. Only one IP address can be associated with an IP interface.

Owner and non-owner configurations must include the following parameters:

- All participating routers in a VRRP instance must be configured with the same *vrid.*
- The *owner* configuration must include at least one backup IP address.

Other owner and non-owner configurations include the following optional commands:

- authentication-key
- message-interval

In addition to the common parameters, the following *non-owner* commands can be configured:

- master-int-inherit
- priority
- policy
- ping-reply
- preempt
- telnet-reply
- ssh-reply (IPv4 only)
- [no] shutdown

Creating Interface Parameters

If you have multiple subnets configured on an Ethernet interface, you can configure VRRP on each subnet.

The following displays an IP interface configuration example:

```
A:SR1>config>router# info
#------------------------------------------
echo "IP Configuration "
#------------------------------------------
        interface "system"
            address 10.10.0.1/32
        exit
        interface "testA"
            address 123.123.123.123/24
        exit
        interface "testB"
            address 10.10.14.1/24
        exit
        router-id 10.10.0.1
#------------------------------------------
A:SR1>config>router#
```

Configuring VRRP Policy Components

The following displays a VRRP policy configuration example:

```
A:SR1>config>vrrp# info
----------------------------------------------
        policy 1
            delta-in-use-limit 50
            priority-event
                port-down 1/1/2
                    hold-set 43200
                    priority 100 delta
                exit
                route-unknown 0.0.0.0/0
                    protocol isis
                exit
            exit
        exit
----------------------------------------------
A:SR1>config>vrrp#
```

Configuring Service VRRP Parameters

VRRP parameters can be configured on an interface in aservice to provide virtual default router support which allows traffic to be routed without relying on a single router in case of failure. VRRP can be configured the following ways:

- Non-Owner VRRP Example on page 149
- Owner Service VRRP on page 150

Non-Owner VRRP Example

The following displays a basic non-owner VRRP configuration example:

```
A:SR2>config>service>ies# info
----------------------------------------------
...
            interface "testing" create
                address 10.10.10.16/24
                sap 1/1/55:0 create
                vrrp 12
                    backup 10.10.10.15
                    policy 1
                                   authentication-key "testabc"
                exit
            exit
            no shutdown
----------------------------------------------
A:SR2>config>service>ies#
```

Owner Service VRRP

The following displays the owner VRRP configuration example:

```
A:SR4>config>router# info
#------------------------------------------
echo "IP Configuration "
#------------------------------------------
...
        interface "test2"
            address 10.10.10.23/24
            vrrp 1 owner
                backup 10.10.10.23
                  authentication-key "testabc"
            exit
        exit
#------------------------------------------
A:SR4>config>router#
```

Configuring Router Interface VRRP Parameters

VRRP parameters can be configured on an interface in an interface to provide virtual default router support which allows traffic to be routed without relying on a single router in case of failure.

VRRP can be configured the following ways:

- Router Interface VRRP Non-Owner on page 151

Router Interface VRRP Non-Owner

The following displays a non-owner interface VRRP configuration example:

```
A:SR2>config># info
#------------------------------------------
      interface "if-test"
            address 10.20.30.40/24
            vrrp 1
                              backup 10.20.30.41
                ping-reply
                telnet-reply
                     authentication-key "testabc"
            exit
        exit
#------------------------------------------
A:SR2>config>#
```

Router Interface VRRP Owner

The following displays router interface owner VRRP configuration example:

```
A:SR2>config>router# info
#------------------------------------------
     interface "vrrpowner"
            address 10.10.10.23/24
            vrrp 1 owner
                backup 10.10.10.23
                authentication-key "testabc"
            exit
        exit
#------------------------------------------
A:SR2>config>router#
```

VRRP Configuration Management Tasks

This section discusses the following VRRP configuration management tasks:

- Modifying a VRRP Policy on page 153
- Deleting a VRRP Policy on page 154
- Modifying Service and Interface VRRP Parameters on page 155
  - → Modifying Non-Owner Parameters on page 155
  - → Modifying Owner Parameters on page 155
  - → Deleting VRRP on an Interface or Service on page 155

Modifying a VRRP Policy

To access a specific VRRP policy, you must specify the policy ID. To display a list of VRRP policies, use the `show vrrp policy` command.

The following example displays the modified VRRP policy configuration:

```
A:SR2>config>vrrp>policy# info
----------------------------------------------
            delta-in-use-limit 50
            priority-event
                port-down 1/1/2
                    hold-set 43200
                    priority 100 delta
                exit
                port-down 1/1/3
                    priority 200 explicit
                exit
                host-unreachable 10.10.24.4
                    drop-count 25
                exit
            exit
----------------------------------------------
A:SR2>config>vrrp>policy#
```

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 interface or to an IES service. Each instance in which the policy is applied must be deleted.

The `Applied` column in the following example displays whether or not the VRRP policies are applied to an entity.

```
A:SR2#
===============================================================================
VRRP Policies
===============================================================================
Policy    Current             Current      Current      Delta       Applied
Id        Priority & Effect   Explicit     Delta Sum    Limit
-------------------------------------------------------------------------------
1        200 Explicit        200          100          50          Yes
15       254                 None         None         1           No
32       100                 None         None         1           No
===============================================================================
A:SR2#
```

Modifying Service and Interface VRRP Parameters

Modifying Non-Owner Parameters

Once a VRRP instance is created as non-owner, it cannot be modified to the `owner` state. The `vrid` must be deleted and then recreated with the `owner` keyword to invoke IP address ownership.

Modifying Owner Parameters

Once a VRRP instance is created as `owner`, it cannot be modified to the non-owner state. The `vrid` must be deleted and then recreated *without* the `owner` keyword to remove IP address ownership.

Entering the `owner` keyword is optional when entering the `vrid` for modification purposes.

Deleting VRRP on an Interface or Service

The *vrid* does not need to be shutdown to remove the virtual router instance from an interface or service.

Example:

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

The following example displays the command usage to delete a VRRP instance from an interface or IES service:

Example:

```
config>service#ies 10
config>service>ies# interface "test"
config>service>ies>if# vrrp 1
config>service>ies>if>vrrp# shutdown
config>service>ies>if>vrrp# exit
config>service>ies>if# no vrrp 1
config>service>ies>if# exit all
```

VRRP Command Reference

Command Hierarchies

Configuration Commands

VRRP Network Interface Commands (Not applicable to 7210 SAS-M in access-uplink mode).

config
— **router**
— [**no**] **interface** *interface-name*
— **address** {*ip-address/mask* | *ip-address netmask*} [**broadcast** *all-ones* | *host-ones*]
— **no address**
— [**no**] **allow-directed-broadcasts**
— **arp-timeout** *seconds*
— **no arp-timeout**
— **description** *description-string*
— **no description**
— [**no**] **shutdown**
— **static-arp** *ip-address ieee-address*
— [**no**] **static-arp** *ip-address*
— **vrrp** *virtual-router-id* [**owner**] *
— **no vrrp** *virtual-router-id*
— **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
— **no authentication-key**
— [**no**] **backup** *ip-address*
— [**no**] **bfd-enable** *service-id* **interface** *interface-name* **dst-ip** *ip-address*
— [**no**] **bfd-enable** **interface** *interface-name* **dst-ip** *ip-address*
— **init-delay** *seconds*
— **no init-delay**
— [**no**] **master-int-inherit**
— **message-interval** {[*seconds*] [**milliseconds** *milliseconds*]}
— **no message-interval**
— [**no**] **ping-reply**
— **policy** *policy-id*
— **no policy**
— [**no**] **preempt**
— **priority** *priority*
— **no priority**
— [**no**] **ssh-reply**
— [**no**] **telnet-reply**
— [**no**] **shutdown**
— [**no**] **traceroute-reply**

.

VRRP Priority Control Event Policy Commands

config
- **vrrp**
  - [**no**] **policy** *policy-id* [**context** *service-id*]
    - **delta-in-use-limit** *limit*
    - **no delta-in-use-limit**
    - **description** *description string*
    - **no description**
    - [**no**] **priority-event**
      - [**no**] **host-unreachable** *ip-address*
        - **drop-count** *consecutive-failures*
        - **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**
      - [**no**] **lag-port-down** *lag-id*
        - **hold-clear** *seconds*
        - **no hold-clear**
        - **hold-set** *seconds*
        - **no hold-set**
        - [**no**] **number-down** *number-of-lag-ports-down*
          - **priority** *priority-level* [**delta** | **explicit**]
          - **no priority**
      - [**no**] **port-down** *port-id*
        - **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*
        - **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**[*protocol*]
— [**no**] **protocol ospf**
— [**no**] **protocol isis**
— [**no**] **protocol static**

Show Commands

show
— **vrrp**
— **policy** [*policy-id* [**event** *event-type specific-qualifier*]]
— **router**
— **vrrp**
— **instance**
— **instance** [**interface** *interface-name* [**vrid** *virtual-router-id*]]
— **statistics**

Monitor Commands

monitor
— **router**
— **vrrp**
— **instance interface** *interface-name* **vr-id** *virtual-router-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Clear Commands

clear
— **vrrp**
— **statistics**
— **router**
— **vrrp**
— **interface** *ip-int-name* [**vrid** *virtual-router-id*]
— **statistics interface** *interface-name* [**vrid** *virtual-router-id*]
— **statistics**

Debug Commands

debug
— **router**
— **vrrp**
— **events**
— **events interface** *ip-int-name* [**vrid** *virtual-router-id*]
— **no events**
— **no events interface** *ip-int-name* [**vrid** *virtual-router-id*]
— **packets**
— **packets interface** *ip-int-name* [**vrid** *virtual-router-id*]
— **packets**
— **no packets**
— **no packets interface** *ip-int-name* [**vrid** *virtual-router-id*]

— **no packets**

Configuration Commands

Interface Configuration Commands

authentication-key

Syntax **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
no authentication-key

Context config>router>if>vrrp

Description This command sets the simple text authentication key used to generate master VRRP advertisement messages and validates VRRP advertisements.

If simple text password authentication is not required, the **authenticaton-key** command is not required.

The command is configurable in both non-owner and owner **vrrp** nodal contexts.

The *key* parameter identifies the simple text password to be used when VRRP Authentication Type 1 is enabled on the virtual router instance. Type 1 uses an eight octet long string that is inserted into all transmitted VRRP advertisement messages and is compared against all received VRRP advertisement messages. The authentication data fields are used to transmit the *key*.

The *key* string is case sensitive and is left justified in the VRRP advertisement message authentication data fields. The first field contains the first four characters with the first octet (starting with IETF RFC bit position 0) containing the first character. The second field similarly holds the fifth through eighth characters. Any unspecified portion of the authentication data field is padded with a 0 value in the corresponding octet.

If the command is re-executed with a different password key defined, the new key is used ediately.

The **authentication-key** command can be executed at anytime.

To change the current in-use password key on multiple virtual router instances:

1. Identify the current master.
2. Shutdown the virtual router instance on all backups.
3. Execute the **authentication-key** command on the master to change the password key.
4. Execute the **authentication-key** command and **no shutdown** command on each backup.

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

Default no authentication-key — The authentication key value is the null string.

Parameters *authentication-key* — The authentication key. Allowed values are any string up to 8 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.

hash-key — The hash key. The key can be any combination of ASCII characters up to 22 (hash-key1) or 121 (hash-key2) characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

backup

Syntax [**no**] **backup** *ip-address*

Context config>router>if>vrrp

Description This command associates router IP addresses with the parental IP interface IP addresses.

The **backup** command has two distinct functions when used in an **owner** or a **non-owner** context of the virtual router instance.

Non-owner virtual router instances actually create a routable IP interface address that is operationally dependent on the virtual router instance mode (master or backup). The **backup** command in **owner** virtual router instances does not create a routable IP interface address; it simply defines the existing parental IP interface IP addresses that are advertised by the virtual router instance.

For **owner** virtual router instances, the **backup** command defines the IP addresses that are advertised within VRRP advertisement messages. This communicates the IP addresses that the master is representing to backup virtual routers receiving the messages. Advertising a correct list is important. The specified *ip-addr* must be equal to the existing parental IP interface IP addresses (primary) or the **backup** command will fail.

For non-owner virtual router instances, the **backup** command actually creates an IP interface IP address used for routing IP packets and communicating with the system when the access commands are defined (**ping-reply**, **telnet-reply**, and **ssh-reply**). The specified *ip-addr* must be an IP address of the parental IP interface local subnets created with the **address** . If a local subnet does not exist that includes the specified *ip-addr* or if *ip-addr* is the same IP address as the parental IP interface IP address, the **backup** command will fail.

The new interface IP address created with the **backup** command assumes the mask and parameters of the corresponding parent IP interface IP address. The *ip-addr* is only active when the virtual router instance is operating in the master state. When not operating as master, the virtual router instance acts as if it is operationally down. It will not respond to ARP requests to *ip-addr*, nor will it route packets received with its *vrid* derived source MAC address. A non-master virtual router instance always silently discards packets destined to *ip-addr*. A single virtual router instance may only have a single virtual router IP address from a given parental local subnet. Multiple virtual router instances can define a virtual router IP address from the same local subnet as long as each is a different IP address.

When operating as (non-owner) master, the default functionality associated with *ip-addr* is ARP response to ARP requests to *ip-addr*, routing of packets destined to the virtual router instance source MAC address and silently discarding packets destined to *ip-addr*. Enabling the non-owner-access parameters selectively allows ping, Telnet and SSH connectivity to *ip-addr* when the virtual router instance is operating as master.

The **no** form of the command removes the specified virtual router IP address from the virtual router instance. For non-owner virtual router instances, this causes all routing and local access associated with the *ip-addr* to cease. For **owner** virtual router instances, the **no backup** command only removes *ip-addr* from the list of advertised IP addresses. If the last *ip-addr* is removed from the virtual router instance, the virtual router instance will enter the operationally down state

Special Cases

Assigning the Virtual Router ID IP Address — Once the *vrid* is created on the parent IP interface, IP addresses need to be assigned to the virtual router instance. If the *vrid* was created with the keyword **owner**, the virtual router instance IP addresses must have the parent IP interface defined IP addresses (primary). For non-owner virtual router instances, the virtual router IP addresses each must be within one of the parental IP interface IP address defined local subnets. For both **owner** and non-owner virtual router instances, the virtual router IP addresses must be explicitly defined using the **backup** *ip-addr* command.

Virtual Router Instance IP Address Assignment Conditions — The RFC does not specify that the assigned IP addresses to the virtual router instance must be in the same subnet as the parent IP interface primary IP address. The only requirement is that all virtual routers participating in the same virtual router instance have the same virtual router IP addresses assigned. To avoid confusion, the assigned virtual router IP addresses must be in a local subnet of one of the parent IP interfaces IP addresses. For **owner** virtual router instances the assigned virtual router IP address must be the same as the parental IP interface primary.

The following rules apply when adding, changing, or removing parental and virtual router IP addresses:

Owner Virtual Router IP Address Parental Association — When an IP address is assigned to an **owner** virtual router instance, it must be associated with one of the parental IP interface-assigned IP addresses. The virtual router IP address must be equal to the primary oIP address within the parental IP interface.

Example - Owner Virtual Router Instance

Parent IP addresses:	10.10.10.10/24	
Virtual router IP addresses:	10.10.10.11	Invalid (not equal to parent IP address)
	10.10.10.10	Associated (same as parent IP address 10.10.10.10)
	10.10.11.11	Invalid (not equal to parent IP address)

Non-Owner Virtual Router IP Address Parental Association — When an IP address is assigned to a non-owner virtual router instance, it must be associated with one of the parental IP interface assigned IP addresses. The virtual router IP address must be a valid IP address within one of the parental IP interfaces local subnet. Local subnets are created by the primary IP address in conjunction with the IP addresses mask. If the defined virtual router IP address is equal to the associated subnet's broadcast address, it is invalid. Virtual router IP addresses for non-owner virtual router instances that are equal to a parental IP interface IP address are also invalid.

The same virtual router IP address may not be assigned to two separate virtual router instances. If the virtual router IP address already exists on another virtual router instance, the virtual router IP address assignment will fail.

Example - Non-Owner Virtual Router Instance

Parent IP addresses:	10.10.10.10/24	
Virtual router IP addresses:	10.10.10.11	Associated with 10.10.10.10 (in subnet)
	10.10.10.10	Invalid (same as parent IP address)
	10.10.11.11	Invalid (outside of all Parent IP subnets)

Virtual Router IP Address Assignment without Parent IP Address — When assigning an IP address to a virtual router instance, an associated IP address (see **Owner Virtual Router IP Address Parental Association** and **Non-Owner Virtual Router IP Address Parental Association**) on the parental IP interface must already exist. If an associated IP address on the parental IP interface is not configured, the virtual router IP address assignment fails.

Parent Primary IP Address Changed — When a virtual router IP address is set and the associated parent IP interface IP address is changed, the new parent IP interface IP address is evaluated to ensure it meets the association rules defined in **Owner Virtual Router IP Address Parental Association** or **Non-Owner Virtual Router IP Address Parental Association**. If the association check fails, the parental IP address change is not allowed. If the parental IP address change fails, the previously configured IP address definition remains in effect.

Only the primary parent IP address can be changed. **Parent Primary IP Address Removal** explains IP address removal conditions.

Parent Primary IP Address Removal — When a virtual router IP address is successfully set, but removing the associated parent IP interface IP address is attempted and fails. All virtual router IP addresses associated with the parental IP interface IP address must be deleted prior to removing the parental IP address. This includes virtual router IP address associations from multiple virtual router instances on the IP interface.

Default no backup — No virtual router IP address is assigned.

Parameters *ip-address* — The virtual router IP address expressed in dotted decimal notation. The IP virtual router IP address must be in the same subnet of the parental IP interface IP address or equal to the primary IP address for **owner** virtual router instances.

Values 1.0.0.1 - 223.255.255.254

bfd-enable

Syntax [**no**] **bfd-enable** [*service-id*] **interface** *interface-name* **dst-ip** *ip-address*
[**no**] **bfd-enable interface** *interface-name* **dst-ip** *ip-address*

Context config>router>if>vrrp

Description This commands assigns a bi-directional forwarding (BFD) session providing heart-beat mechanism for the given VRRP instance. There can be only one BFD session assigned to any given VRRP instance, but there can be multiple VRRP sessions using the same BFD session.

BFD control the state of the associated interface. By enabling BFD on a given 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. The parameters used for the BFD are set by the BFD command under the IP interface. The specified interface may not be configured with BFD; when it is, the virtual router will then initiate the BFD session.

The **no** form of this command removes BFD from the configuration.

Default none

Parameters *service-id* — Specifies the service ID of the interface running BFD.

Values *service-id*: 1 — 2147483647
svc-name: 64 characters maximum

interface *interface-name* **—** Specifies the name of the interface running BFD. The specified interface may not yet be configured with BFD. However, when it is, this virtual router will then initiate the BFD session.

dst-ip *ip-address* **—** Specifies the destination address to be used for the BFD session.

init-delay

Syntax **init-delay** *seconds*
no init-delay

Context config>router>if>vrrp

Description This command configures a VRRP initialization delay timer.

Parameters *seconds* — Specifies the initialization delay timer for VRRP, in seconds.

Values 1 — 65535

master-int-inherit

Syntax [**no**] **master-int-inherit**

Context config>router>if>vrrp

Description This command enables the virtual router instance to inherit the master VRRP router's advertisement interval timer which is used by backup routers to calculate the master down timer.

The **master-int-inherit** command is only available in the non-owner nodal context and is used to allow the current virtual router instance master to dictate the master down timer for all backup virtual routers. The **master-int-inherit** command has no effect when the virtual router instance is operating as master.

If **master-int-inherit** is not enabled, the locally configured **message-interval** must match the master's VRRP advertisement message advertisement interval field value or the message is discarded.

The **no** form of the command restores the default operating condition which requires the locally configured **message-interval** to match the received VRRP advertisement message advertisement interval field value.

Default no master-int-inherit — The virtual router instance does not inherit the master VRRP router's advertisement interval timer and uses the locally configured message interval.

message-interval

Syntax **message-interval** {[*seconds*] [**milliseconds** *milliseconds*]}
no message-interval

Context config>router>if>vrrp

Description This command configures the administrative advertisement message timer used by the master virtual router instance to send VRRP advertisement messages and to derive the master down timer as backup.

For an owner virtual router instance, the administrative advertisement timer directly sets the operational advertisement timer and indirectly sets the master down timer for the virtual router instance.

Non-owner virtual router instances usage of the **message-interval** setting is dependent on the state of the virtual router (master or backup) and the state of the **master-int-inherit** parameter.

- When a non-owner is operating as master for the virtual router, the configured **message-interval** is used as the operational advertisement timer similar to an owner virtual router instance. The **master-int-inherit** command has no effect when operating as master.
- When a non-owner is in the backup state with **master-int-inherit** disabled, the configured **message-interval** value is used to match the incoming VRRP advertisement message advertisement interval field. If the locally configured message interval does not match the advertisement interval field, the VRRP advertisement is discarded.

- When a non-owner is in the backup state with **master-int-inherit** enabled, the configured **message-interval** is ignored. The master down timer is indirectly derived from the incoming VRRP advertisement message advertisement interval field value.

VRRP advertisements messages that are fragmented contain IP options (IPv4) require a longer message interval to be configured.

The in-use value of the message interval is used to derive the master down timer to be used when the virtual router is operating in backup mode based on the following formula:

(3x (in-use message interval) + skew time)

The skew time portion is used to slow down virtual routers with relatively low priority values when competing in the master election process.

The command is available in both non-owner and owner **vrrp** nodal contexts.

By default, a **message-interval** of 1 second is used.

In 7210, the least timer values supported is 1 second. Timers less than 1 second cannot be used.

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

Default 1 — Advertisement timer set to 1 second

Parameters *seconds* — The number of seconds that will transpire before the advertisement timer expires expressed as a decimal integer.

Values IPv4: 1 — 255

milliseconds *milliseconds* **—** Specifies the time interval, in milliseconds, between sending advertisement messages.

Values 100 — 900

policy

Syntax **policy** *policy-id*
no policy

Context config>router>if>vrrp

Description This command adds a VRRP priority control policy association with the virtual router instance.

To further augment the virtual router instance base priority, VRRP priority control policies can be used to override or adjust the base priority value depending on events or conditions within the chassis.

The policy can be associated with more than one virtual router instance. The priority events within the policy either override or diminish the base priority set with the **priority** command dynamically affecting the in-use priority. As priority events clear in the policy, the in-use priority can eventually be restored to the base **priority** value.

The **policy** command is only available in the non-owner **vrrp** nodal context. The priority of **owner** virtual router instances is permanently set to 255 and cannot be changed by VRRP priority control policies. For non-owner virtual router instances, if the **policy** command is not executed, the base **priority** is used as the in-use priority.

The **no** form of the command removes existing VRRP priority control policy associations from the virtual router instance. All associations must be removed prior to deleting the policy from the system.

Default no policy — No VRRP priority control policy is associated with the virtual router instance.

Parameters *policy-id* — The policy ID of the VRRP priority control expressed as a decimal integer. The *vrrp-policy-id* must already exist for the command to function.

Values 1 — 9999

preempt

Syntax [**no**] **preempt**

Context config>router>if>vrrp

Description This command enables the overriding of an existing VRRP master if the virtual router's in-use priority is higher than the current master.

The priority of the non-owner virtual router instance, the preempt mode allows the best available virtual router to force itself as the master over other available virtual routers.

When **preempt** is enabled, the virtual router instance overrides any non-owner master with an in-use message priority value less than the virtual router instance in-use priority value. If **preempt** is disabled, the virtual router only becomes master if the master down timer expires before a VRRP advertisement message is received from another virtual router.

Enabling **preempt** mode improves the effectiveness of the base **priority** and the VRRP priority control policy mechanisms on the virtual router instance. If the virtual router cannot preempt an existing non-owner master, the affect of the dynamic changing of the in-use priority is diminished.

The **preempt** command is only available in the non-owner **vrrp** nodal context. The owner may not be preempted because the priority of non-owners can never be higher than the owner. The owner always preempts all other virtual routers when it is available.

Non-owner virtual router instances only preempt when **preempt** is set and the current master has an in-use message priority value less than the virtual router instances in-use priority.

A master non-owner virtual router only allows itself to be preempted when the incoming VRRP advertisement message priority field value is one of the following:

- Greater than the virtual router in-use priority value.
- Equal to the in-use priority value and the source IP address (primary IP address) is greater than the virtual router instance primary IP address.

By default, preempt mode is enabled on the virtual router instance.

The **no** form of the command disables preempt mode and prevents the non-owner virtual router instance from preempting another, less desirable virtual router.

Default **preempt** — The preempt mode enabled on the virtual router instance where it will preempt a VRRP master with a lower priority.

priority

Syntax **priority** *base-priority*
no priority

Context config>router>if>vrrp

Description This command configures the base router priority for the virtual router instance used in the master election process.

The priority is the most important parameter set on a non-owner virtual router instance. The priority defines a virtual router's selection order in the master election process. Together, the priority value and the **preempt** mode allow the virtual router with the best priority to become the master virtual router.

The *base-priority* is used to derive the in-use priority of the virtual router instance as modified by any optional VRRP priority control policy. VRRP priority control policies can be used to either override or adjust the base priority value depending on events or conditions within the chassis.

The **priority** command is only available in the non-owner **vrrp** nodal context. The priority of **owner** virtual router instances is permanently set to 255 and cannot be changed.

For non-owner virtual router instances, the default base priority value is 100.

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

Default **100**

Parameters *base-priority* — The base priority used by the virtual router instance expressed as a decimal integer. If no VRRP priority control policy is defined, the *base-priority* is the in-use priority for the virtual router instance.

Values 1 — 254

ping-reply

Syntax [**no**] **ping-reply**

Context config>router>if>vrrp

Description This command enables the non-owner master to reply to ICMP echo requests directed at the vritual router instances IP addresses.

Non-owner virtual router instances are limited by the VRRP specifications to responding to ARP requests destined to the virtual router IP addresses and routing IP packets not addressed to the virtual router IP addresses. Many network administrators find this limitation frustrating when troubleshooting VRRP connectivity issues.

allows this access limitation to be selectively lifted for certain applications. Ping, Telnet and SSH can be individually enabled or disabled on a per-virtual-router-instance basis.

The **ping-reply** command enables the non-owner master to reply to ICMP echo requests directed at the virtual router instances IP addresses. The Ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parental IP interface or based on the Ping source host address).

When **ping-reply** is not enabled, ICMP echo requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP echo requests regardless of the **ping-reply** setting.

The **ping-reply** command is only available in non-owner **vrrp** nodal context.

By default, ICMP echo requests to the virtual router instance IP addresses are silently discarded.

The **no** form of the command configures discarding all ICMP echo request messages destined to the non-owner virtual router instance IP addresses.

Default **no ping-reply** — ICMP echo requests to the virtual router instance IP addresses are discarded.

shutdown

Syntax [**no**] **shutdown**

Context config>router>if>vrrp

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command administratively enables an entity.

Special Cases **Non-Owner Virtual Router —** Non-owner virtual router instances can be administratively shutdown. This allows the termination of VRRP participation in the virtual router and stops all routing and other access capabilities with regards to the virtual router IP addresses. Shutting down the virtual router instance provides a mechanism to maintain the virtual routers without causing false backup/master state changes.

If the **shutdown** command is executed, no VRRP advertisement messages are generated and all received VRRP advertisement messages are silently discarded with no processing.

By default, virtual router instances are created in the **no shutdown** state.

Whenever the administrative state of a virtual router instance transitions, a log message is generated.

Whenever the operational state of a virtual router instance transitions, a log message is generated.

Owner Virtual Router — An owner virtual router context does not have a **shutdown** command. To administratively disable an owner virtual router instance, use the **shutdown** command within the parent IP interface node which administratively downs the IP interface.

ssh-reply

Syntax [**no**] **ssh-reply**

Context config>router>if>vrrp

Description This command enables the non-owner master to reply to SSH requests directed at the virtual router instance IP addresses. This command is only applicable to IPv4.

Non-owner virtual router instances are limited by the VRRP specifications to responding to ARP requests destined to the virtual router IP addresses and routing IP packets not addressed to the virtual router IP addresses.

This limitation can be disregarded for certain applications. Ping, Telnet and SSH can be individually enabled or disabled on a per-virtual-router-instance basis.

The **ssh-reply** command enables the non-owner master to reply to SSH requests directed at the virtual router instances IP addresses. The SSH request can be received on any routed interface. SSH must not have been disabled at the management security level (either on the parental IP interface or based on the SSH source host address). Proper login and CLI command authentication is still enforced.

When **ssh-reply** is not enabled, SSH requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to SSH requests regardless of the **ssh-reply** setting.

The **ssh-reply** command is only available in non-owner **vrrp** nodal context.

By default, SSH requests to the virtual router instance IP addresses are silently discarded.

The **no** form of the command discards all SSH request messages destined to the non-owner virtual router instance IP addresses.

Default **no ssh-reply** — SSH requests to the virtual router instance IP addresses are discarded.

telnet-reply

Syntax [**no**] **telnet-reply**

Context config>router>if>vrrp

Description This command enables the non-owner master to reply to TCP port 23 Telnet requests directed at the virtual router instances' IP addresses.

Non-owner virtual router instances are limited by the VRRP specifications to responding to ARP requests destined to the virtual router IP addresses and routing IP packets not addressed to the virtual router IP addresses. Many network administrators find this limitation frustrating when troubleshooting VRRP connectivity issues.

This limitation can be disregarded for certain applications. Ping, SSH and Telnet can each be individually enabled or disabled on a per-virtual-router-instance basis.

The **telnet-reply** command enables the non-owner master to reply to Telnet requests directed at the virtual router instances' IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Proper login and CLI command authentication is still enforced.

When **telnet-reply** is not enabled, Telnet requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet requests regardless of the **telnet-reply** setting.

The **telnet-reply** command is only available in non-owner **vrrp** nodal context.

By default, Telnet requests to the virtual router instance IP addresses will be silently discarded.

The **no** form of the command configures discarding all Telnet request messages destined to the non-owner virtual router instance IP addresses.

Default **no telnet-reply** — Telnet requests to the virtual router instance IP addresses are discarded.

traceroute-reply

Syntax [**no**] **traceroute-reply**

Context config>router>if>vrrp

Description This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the **trace-route-reply** status.

Default no traceroute-reply

vrrp

Syntax **vrrp** *vrid* [**owner**]
no vrrp *vrid*

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

Description This command creates the context to configure a VRRP virtual router instance. A virtual router is defined by its virtual router identifier (VRID) and a set of IP addresses.

The optional **owner** keyword indicates that the **owner** controls the IP address of the virtual router and is responsible for forwarding packets sent to this IP address. The **owner** assumes the role of the master virtual router.

All other virtual router instances participating in this message domain must have the same *vrid* configured and cannot be configured as **owner**. Once created, the **owner** keyword is optional when entering the *vrid* for configuration purposes.

A *vrid* is internally associated with the IP interface. This allows the *vrid* to be used on multiple IP interfaces while representing different virtual router instances.

For IPv4, up to four **vrrp** *vrid* nodes can be configured on a router interface. Each virtual router instance can manage up to 16 backup IP addresses.

The **no** form of the command removes the specified *vrid* from the IP interface. This terminates VRRP participation and deletes all references to the *vrid* in conjunction with the IP interface. The *vrid* does not need to be shutdown to remove the virtual router instance.

Special Cases

Virtual Router Instance Owner IP Address Conditions — It is possible for the virtual router instance **owner** to be created prior to assigning the parent IP interface primary IP address. When this is the case, the virtual router instance is not associated with an IP address. The operational state of the virtual router instance is down.

VRRP Owner Command Exclusions — By specifying the VRRP *vrid* as **owner**, The following commands are no longer available:

- **vrrp priority —** The virtual router instance **owner** is hard-coded with a **priority** value of 255 and cannot be changed.
- **vrrp master-int-inherit** — Owner virtual router instances do not accept VRRP advertisement messages; the advertisement interval field is not evaluated and cannot be inherited.
- **ping-reply**, **telnet-reply** and **ssh-reply —** The **owner** virtual router instance always allows Ping, Telnet and SSH if the management and security parameters are configured to accept them on the parent IP interface.
- **vrrp shutdown —** The **owner** virtual router instance cannot be shutdown in the **vrrp** node. If this was allowed, VRRP messages would not be sent, but the parent IP interface address would continue to respond to ARPs and forward IP packets. Another virtual router instance may detect the missing master due to the termination of VRRP advertisement messages and become master. This would cause two routers responding to ARP requests for the same IP addresses. To **shutdown** the **owner** virtual router instance, use the **shutdown** command in the parent IP interface context. This will prevent VRRP participation, IP ARP reply and IP forwarding. To continue parent IP interface ARP reply and forwarding without VRRP participation, remove the **vrrp** *vrid* instance.
- traceroute-reply

Default

no vrrp — No VRRP virtual router instance is associated with the IP interface.

Parameters

vrid — The virtual router ID for the IP interface expressed as a decimal integer.

Values 1 — 255

owner — Identifies this virtual router instance as owning the virtual router IP addresses. If the **owner** keyword is not specified at the time of *vrid* creation, the **vrrp backup** commands must be specified to define the virtual router IP addresses. The **owner** keyword is not required when entering the *vrid* for editing purposes. Once created as **owner**, a *vrid* on an IP interface cannot have the **owner** parameter removed. The *vrid* must be deleted and than recreated without the **owner** keyword to remove ownership.

Priority Policy Commands

delta-in-use-limit

Syntax **delta-in-use-limit** *in-use-priority-limit*
no delta-in-use-limit

Context config>vrrp>policy *vrrp-policy-id*

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.

Changing the *in-use-priority-limit* causes an ediate 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** — The lower limit of 1 for the in-use priority, as modified, by delta priorty control events.

Parameters *in-use-priority-limit* — The lower limit of the in-use priority base, as modified by priority control policies. The *in-use-priority-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 instances base-priority, is less than the *in-use-priority-limit*, the *in-use-priority-limit* value is used as the virtual router instances in-use priority value.

Setting the *in-use-priority-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.

Values 1 — 254

description

Syntax **description** *string*
no description

Context config>vrrp>policy *vrrp-policy-id*

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

The **description** 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 none

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

policy

Syntax **policy** *policy-id* [**context** *service-id*]
no policy *policy-id*

Context config>vrrp

Description This command creates the context to configure a VRRP priority control policy which is used to control the VRRP in-use priority based on priority control events. It is a parental node for the various VRRP priority control policy commands that define the 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 or diminish the base priority setting to establish the actual in-use priority of the virtual router instance.

The **policy** *policy-id* command must be created first, before it can be associated with a virtual router instance.

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 1000.

The *policy-id* 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 will fail.

Default none

Parameters *vrrp-policy-id* — The VRRP priority control ID expressed as a decimal integer that uniquely identifies this policy from any other VRRP priority control policy defined on the system. Up to 1000 policies can be defined.

Values 1 — 9999

context *service-id* **—** Specifies the service ID to which this policy applies. A value of zero (0) means that this policy does not apply to a service but applies to the base router instance.

Values 1 — 2147483647

priority-event

Syntax [**no**] **priority-event**

Context config>vrrp>policy *vrrp-priority-id*

Description This command creates 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 within the **priority-event** node.

The **no** form of the command clears any configured priority events.

Priority Policy Event Commands

hold-clear

Syntax **hold-clear** *seconds*
no hold-clear

Context config>vrrp>policy>priority-event>port-down
config>vrrp>policy>priority-event>lag-port-down
config>vrrp>policy>priority-event>route-unknown

Description This command configures the hold clear time for the event. The *seconds* parameter specifies the hold-clear time, the amount of time in seconds by which the effect of a cleared event on the associated virtual router instance is delayed.

The hold-clear time is used to prevent black hole conditions when 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 — 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 event can transition to the cleared state to dampen flapping events. A flapping event continually transitions between clear and set.

The **hold-set** command is used to dampen the effect of a flapping event. The **hold-set** value is loaded into a hold set timer that prevents a set event from transitioning to the cleared state until it expires.

Each time an event transitions between cleared and set, the timer is loaded and begins a countdown to zero. When the timer reaches zero, 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 reload the hold-set timer. This extends the amount of time that must expire before entering the cleared state.

Once the hold set timer expires and the event meets the cleared state requirements or is set to a lower threshold, the current set effect on the virtual router instances in-use priority can be removed. As with **lag-port-down** events, this may be a decrease in the set effect if the *clearing* amounts to a lower set threshold.

The **hold-set** command can be executed at anytime. If the hold-set timer value is configured larger than the new *seconds* setting, the timer is loaded with the new **hold-set** value.

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

Default 0 — The hold-set timer is disabled so event transitions are processed ediately.

Parameters *seconds* — 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 — 86400

priority

Syntax **priority** *priority-level* [{**delta** | **explicit**}]
no priority

Context config>vrrp>policy>priority-event>host-unreachable *ip-addr*
config>vrrp>policy>priority-event>lag-port-down *lag-id*>number-down *number-of-lag-ports-down*
config>vrrp>policy>priority-event>port-down *port-id*[.*channel-id*]
config>vrrp>policy>priority-event>route-unknown *prefix*/*mask-length*

Description This command controls the effect 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** keywords are 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 that are 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 delta priorities sum exceeds the **delta-in-use-limit** parameter, then the **delta-in-use-limit** parameter 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**, thus, there is no impact on the in-use priority.

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

Default 0 delta — The set event will subtract 0 from the base priority (no effect).

Parameters *priority-level* — The priority level adjustment value expressed as a decimal integer.

Values 0 — 254

delta | explicit — Configures what effect the *priority-level* will have on the base priority value.

When **delta** is specified, the *priority-level* value is subtracted from the associated virtual router instance's base priority 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**

Values delta, explicit

Priority Policy Port Down Event Commands

port-down

Syntax [**no**] **port-down** *port-id*

Context config>vrrp>policy>priority-event

Description This command configures a port down priority control event that monitors the operational state of a port or SONET/SDH channel. When the port or channel enters the operational down state, the event is considered set. When the port or channel enters the operational up state, the event is considered cleared.

Multiple unique **port-down** event nodes can be configured within the **priority-event** context up to the overall limit of 32 events. Up to 32 events can be defined in any combination of types.

The **port-down** command can reference an arbitrary port or channel. The port or channel does not need to be pre-provisioned or populated within the system. The operational state of the **port-down** event will indicate:

- Set – non-provisioned
- Set – not populated
- Set – down
- Cleared – up

When the port or channel 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 ediately and must be reflected in the associated virtual router instances in-use priority value. As the event transitions from cleared 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.

When the event enters the operationally up state, the event is considered to be cleared. Once the events **hold-set** expires, the effects of the events **priority** value are ediately 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 or channel monitoring event. The event may be removed at anytime. When the event is removed, the in-use priority of all associated virtual router instances will be re-evaluated. The events **hold-set** timer has no effect on the removal procedure.

Default **no port-down** — No port down priority control events are defined.

Parameters *port-id* — The port ID of the port monitored by the VRRP priority control event.

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. A port and a specific channel on the port are considered to be separate entities. A port and a channel on the port can be monitored by separate events in the same policy.

Values port-id *slot*/*mda*/*port*[.*channel*]

The POS channel on the port monitored by the VRRP priority control event. The *port-id***.***channel-id* can only be monitored by a single event in this policy. The channel can be monitored by multiple VRRP priority control policies. A port and a specific channel on the port are considered to be separate entities. A port and a channel on the port can be monitored by separate events in the same policy.

If the port is provisioned, but the *channel* does not exist or the port has not been populated, the appropriate event operational state is Set – non-populated.

If the port is not provisioned, the event operational state is Set – non-provisioned.

If the POS interface is configured as a clear-channel, the *channel-id* is 1 and the channel bandwidth is the full bandwidth of the port.

Priority Policy LAG Events Commands

lag-port-down

Syntax [**no**] **lag-port-down** *lag-id*

Context config>vrrp>policy>priority-event

Description This command creates 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 operational down state, the event is considered to be set. When all the ports enter the operational 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 an arbitrary LAG. The *lag-id* does have to already 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
- Cleared – all ports up

When the *lag-id* is created, or a port in *lag-id* becomes operationally up or down, the event operational state must be 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 ediately and must be reflected in the associated virtual router instances 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 totally configurable, as more ports go down, the effect on the associated virtual router instances in-use priority is expected to increase (lowering the priority). When each configured threshold is crossed, any higher thresholds are considered further event sets and are processed ediately 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 then previously), the priority effect of the event is not processed until the hold set timer expires. If the number of ports 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 increase, the **number-down** *ports-down* node that expresses a value equal to or less than the number of down ports describes 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 anytime. When the event is removed, the in-use priority of all associated virtual router instances must be reevaluated. The events **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* — 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.

number-down

Syntax [**no**] **number-down** *number-of-lag-ports-down*

Context config>vrrp>policy>priority-event>lag-port-down *lag-id*

Description This command creates a 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 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* — 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 — 4

Priority Policy Host Unreachable Event Commands

drop-count

Syntax **drop-count** *consecutive-failures*
no drop-count

Context config>vrrp *vrrp-policy-id*>priority-event>host-unreachable *ip-addr*

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's consecutive message drop counter. With each successful attempt, the event's consecutive message drop counter resets to zero.

If the event's consecutive message drop counter reaches the **drop-count** value, the **host-unreachable** priority event enters the set state.

The event's **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 zero (expired).

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

Default 3 — 3 consecutive ICMP echo request failures are required before the host unreachable priority control event is set.

Parameters *consecutive-failures* — The number of ICMP echo request message attempts that must fail for the event to enter the set state. It also defines the threshold so a lower consecutive number of failures can clear the event state.

Values 1 — 60

host-unreachable

Syntax [**no**] **host-unreachable** *ip-address*

Context config>vrrp>policy>priority-event

Description This command creates 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.

Multiple unique (different *ip-address*) **host-unreachable** event nodes can be configured within the **priority-event** node to a maximum of 32 events.

The **host-unreachable** command can reference any valid local or remote IP address. The ability to ARP 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-addr* for **drop-count** consecutive attempts. Only applies when IP address is considered local.
Set – no route	No route exists for *ip-addr* for **drop-count** consecutive attempts. Only 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-addr* - not enough failed attempts to set the event.
Cleared – no route	No route exists for *ip-addr* - 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 its cleared and set orientation from the historical success rate. The informational portion of the operational state is derived from the last attempt's result. 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 ediately and must be reflected in the associated virtual router instances 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 hold-set timer be expired 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 may be deleted at anytime. When the event is deleted, the in-use priority of all associated virtual router instances must be reevaluated. The event's **hold-set** timer has no effect on the removal procedure.

Default **no host-unreachable** — No host unreachable priority events are created.

Parameters *ip-addr* — The IP address of the host for which the specific event will monitor connectivity. The *ip-addr* 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 multiple **ping** requests. Each VRRP priority control **host-unreachable** and **ping** destined to the same *ip-addr* 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

interval

Syntax **interval** *seconds*
no interval

Context config>vrrp *vrrp-policy-id*>priority-event>host-unreachable *ip-addr*

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 the command reverts to the default value.

Default 1

Parameters *seconds* — The number of seconds between the ICMP echo request messages sent to the host IP address for the host unreachable priority event.

Values 1 — 60

timeout

Syntax **timeout** *seconds*
no timeout

Context config>vrrp *vrrp-policy-id*>priority-event>host-unreachable *ip-addr*

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 may 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 may 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 loaded with the **timeout** value. 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 that it is possible for a required ARP request to succeed or timeout 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 increments the consecutive message drop counter 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* — The number of seconds 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 — 60

Priority Policy Route Unknown Event Commands

less-specific

Syntax [**no**] **less-specific** [**allow-default**]

Context config>vrrp>policy>priority-event>route-unknown *prefix/mask-length*

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. Specifying **less-specific** allows a CIDR shortest match hit on a route prefix that contains the IP route prefix.

The **less-specific** command eases the RTM lookup criteria when searching for the *prefix/mask-length*. When the **route-unknown** priority event sends the prefix to the RTM (as if it was a destination lookup), the result route table 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. When **less-specific** is not specified, a less specific route table prefix fails to match the configured prefix. The **allow-default** optional parameter 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.

Default no less-specific — The route unknown priority events requires an exact prefix/mask match.

Parameters **allow-default —** When the **allow-default** parameter is specified with the **less-specific** command, an RTM return of 0.0.0.0 matches the IP prefix. If **less-specific** is entered without the **allow-default** parameter, a return of 0.0.0.0 will not match the IP prefix. To disable **allow-default**, but continue to allow **less-specific** match operation, only enter the **less-specific** command (without the **allow-default** parameter).

next-hop

Syntax [**no**] **next-hop** *ip-address*

Context config>vrrp>policy>priority-event>route-unknown *prefix/mask-length*

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-address*, 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.

When more than one next hop IP addresses are 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 error, but continues to execute if part of an **exec** script.

Default no next-hop — No next hop IP address for the route unknown priority control event is defined.

Parameters *ip-address* — The IP address for an acceptable next hop IP address for a returned route prefix from the RTM when looking up the **route-unknown** route prefix.

ipv4-address :a.b.c.d

protocol

Syntax **protocol** {**ospf** | **is-is** | **static**}
no protocol

Context config>vrrp>policy>priority-event>route-unknown *prefix/mask-length*

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 will not include the source of the prefix. The **protocol** command cannot be executed without at least one associated route source parameter. All parameters are reset each time the **protocol** 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 — No route source for the route unknown priority event is defined.

Parameters **ospf —** This parameter 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** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **ospf** parameter, a returned route prefix with a source of OSPF will not be considered a match and will cause the event to enter the set state.

is-is — This parameter 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 **is-is** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **is-is** parameter, a returned route prefix with a source of IS-IS will not be considered a match and will cause the event to enter the set state.

static — This parameter 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** parameter is not exclusive from the other available **protocol** parameters. If **protocol** is executed without the **static** parameter, a returned route prefix with a source of static route will not be considered a match and will cause the event to enter the set state.

route-unknown

Syntax [**no**] **route-unknown** *prefix/mask-length*

Context config>vrrp>policy>priority-event

Description This command creates a 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 Route Table Manager (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.

The command creates a **route-unknown** node identified by *prefix/mask-length* and containing event control commands.

Multiple unique (different *prefix/mask-length*) **route-unknown** event nodes can be configured within the **priority-event** node up to the maximum limit of 32 events.

The **route-unknown** command can reference any valid IP addres 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 does is not an exact match and does not meet any **less-specific** requirements.

route-unknown Operational State	Description
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 may be less specific (the defined prefix may be contained in a larger prefix according to Classless Inter-Domain Routing (CIDR) techniques) if the event has the **less-specific** statement defined. The less specific route that incorporates the router prefix may be the default route (0.0.0.0) if the **less-specific allow-default** statement is defined. The matching prefix may 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 may 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.

When an event transitions from clear to set, the set is processed ediately and must be reflected in the associated virtual router instances 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 **no** form of the command is used to remove the specific *prefix/mask-length* monitoring event. The event can be removed at anytime. When the event is removed, the in-use priority of all associated virtual router instances must be reevaluated. The events **hold-set** timer has no effect on the removal procedure.

Default **no route-unknown** — No route unknown priority control events are defined for the priority control event policy.

Parameters *prefix* — The IP prefix address to be monitored by the route unknown priority control event in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255

mask-length — The subnet mask length expressed as a decimal integer associated with the IP *prefix* defining the route prefix to be monitored by the route unknown priority control event.

Values 0 — 32

ip-address — The IP address of the host for which the specific event will monitor connectivity. The *ip-addr* 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 multiple **ping** requests. Each VRRP priority control **host-unreachable** and **ping** destined to the same *ip-addr* 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	*ip-prefix/mask*:	ip-prefix	a.b.c.d (host bits must be 0)
		mask	0 — 32

Show Commands

instance

Syntax **instance**
instance [**interface** *interface-name* [**vrid** *virtual-router-id*]

Context show>vrrp

Description This command displays information for VRRP instances.

If no command line options are specified, summary information for all VRRP instances displays.

Parameters **interface** *ip-int-name* — Displays detailed information for the VRRP instances on the specified IP interface including status and statistics.

Default Summary information for all VRRP instances.

vrid *virtual-router-id* — Displays detailed information for the specified VRRP instance on the IP interface.

Default All VRIDs for the IP interface.

Values 1 — 255

Output **VRRP Instance Output —** The following table describes the instance command output fields for VRRP.

Label	Description
`Interface name`	The name of the IP interface.
`VR ID`	The virtual router ID for the IP interface
`Own` `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.
`Adm`	`Up` — Indicates that the administrative state of the VRRP instance is up.
	`Down` — Indicates that the administrative state of the VRRP instance is down.
`Opr`	`Up` — Indicates that the operational state of the VRRP instance is up.
	`Down` — Indicates that the operational state of the VRRP instance is down.

Label	Description (Continued)
State	When owner, **backup** defines the IP addresses that are advertised within VRRP advertisement messages. When non-owner, **backup** actually creates an IP interface IP address used for routing IP packets and communicating with the system when the access commands are defined (ping-reply, telnet-reply, and ssh-reply).
Pol Id	The value that uniquely identifies a Priority Control Policy.
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.
InUse Priority	The current in-use priority associated with the VRRP virtual router instance.
Msg Int	The administrative advertisement message timer used by the master virtual router instance to send VRRP advertisement messages and to derive the master down timer as backup.
Inh Int	`Yes` — When the VRRP instance is a non-owner and is operating as a backup and the **master-int-inherit** command is enabled, the master down timer is indirectly derived from the value in the advertisement interval field of the VRRP message received from the current master. `No` — When the VRRP instance is operating as a backup and the **master-int-inherit** command is *not* enabled, the configured advertisement interval is matched against the value in the advertisement interval field of the VRRP message received from the current master. If the two values do not match then the VRRP advertisement is discarded. If the VRRP instance is operating as a master, this value has no effect.
Backup Addr	The backup virtual router IP address.
BFD	Indicates BFD is enabled.
VRRP State	Specifies whether the VRRP instance is operating in a master or backup state.
Policy ID	The VRRP priority control policy associated with the VRRP virtual router instance. A value of 0 indicates that no control policy policy is associated with the virtual router instance.
Preempt Mode	`Yes` — The preempt mode is enabled on the virtual router instance where it will preempt a VRRP master with a lower priority. `No` — The preempt mode is disabled and prevents the non-owner virtual router instance from preempting another, less desirable virtual router.

Label	Description (Continued)
Ping Reply	Yes — A non-owner master is enabled to reply to ICMP Echo requests directed to the virtual router instance IP addresses. Ping Reply is valid only if the VRRP virtual router instance associated with this entry is a non-owner. A non-owner backup virtual router never responds to such ICMP echo requests irrespective if Ping Reply is enabled. No — ICMP echo requests to the virtual router instance IP addresses are discarded.
Telnet Reply	Yes — Non-owner masters can to reply to TCP port 23 Telnet requests directed at the virtual router instances IP addresses. No — Telnet requests to the virtual router instance IP addresses are discarded.
SSH Reply	Yes — Non-owner masters can to reply to SSH requests directed at the virtual router instances IP addresses. No — All SSH request messages destined to the non-owner virtual router instance IP addresses are discarded.
Primary IP of Master	The IP address of the VRRP master.
Primary IP	The IP address of the VRRP owner.
Up Time	The date and time when the operational state of the event last changed.
Virt MAC Addr	The virtual MAC address used in ARP responses when the VRRP virtual router instance is operating as a master.
Auth Type	Specifies the VRRP authentication Type 0 (no authentication), Type 1 (simple password), or Type 2 (MD5) for the virtual router.
Addr List Mismatch	Specifies whether a trap was generated when the IP address list received in the advertisement messages received from the current master did not match the configured IP address list. This is an edge triggered notification. A second trap will not be generated for a packet from the same master until this event has been cleared.
Master Priority	The priority of the virtual router instance which is the current master.
Master Since	The date and time when operational state of the virtual router changed to master. For a backup virtual router, this value specifies the date and time when it received the first VRRP advertisement message from the virtual router which is the current master.

Sample Output

```
*A:ALA-A# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                 VR Id Own Adm  State       Base Pri   Msg Int
                               IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
n2                             1     No  Up   Master       100       1
                               IPv4      Up   n/a         100        No
  Backup Addr: 5.1.1.10
-------------------------------------------------------------------------------
Instances : 2
===============================================================================
*A:ALA-A#


*A:ALA-A# show router vrrp instance interface n2 vrid 1
===============================================================================
VRRP Instance 1 for interface "n2"
===============================================================================
Owner               : No                    VRRP State        : Master
Primary IP of Master: 5.1.1.2 (Self)
Primary IP          : 5.1.1.2               Standby-Forwarding: Disabled
VRRP Backup Addr    : 5.1.1.10
Admin State         : Up                    Oper State        : Up
Up Time             : 09/23/2004 06:53:45 Virt MAC Addr     : 00:00:5e:00:01:01
Auth Type           : None
Config Mesg Intvl   : 1                     In-Use Mesg Intvl : 1
Master Inherit Intvl: No
Base Priority       : 100                   In-Use Priority   : 100
Policy ID           : n/a                   Preempt Mode      : Yes
Ping Reply          : No                    Telnet Reply      : No
SSH Reply           : No                    Traceroute Reply  : No
Init Delay          : 0                     Init Timer Expires: 0.000 sec
Creation State      : Active
-------------------------------------------------------------------------------
Master Information
-------------------------------------------------------------------------------
Primary IP of Master: 5.1.1.2 (Self)
Addr List Mismatch  : No                    Master Priority   : 100
Master Since        : 09/23/2004 06:53:49
-------------------------------------------------------------------------------
Masters Seen (Last 32)
-------------------------------------------------------------------------------
Primary IP of Master   Last Seen             Addr List Mismatch     Msg Count
-------------------------------------------------------------------------------
5.1.1.2                09/23/2004 06:53:49   No                             0
-------------------------------------------------------------------------------
Statistics
-------------------------------------------------------------------------------
Become Master       : 1                     Master Changes    : 1
Adv Sent            : 103                   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
===============================================================================
*A:ALA-A#
```

policy

Syntax **policy** [*vrrp-policy-id* [**event** *event-type specific-qualifier*]]

Context show>vrrp

Description This command displays VRRP priority control policy information.

If no command line options are specified, a summary of the VRRP priority control event policies displays.

Parameters *vrrp-policy-id* — Displays information on the specified priority control policy ID.

Default All VRRP policies IDs

Values 1 — 9999

event *event-type* — Displays information on the specified VRRP priority control event within the policy ID.

Default All event types and qualifiers

Values **port-down** *port-id*
lag-port-down *lag-id*
host-unreachable *host-ip-addr*
route-unknown *route-prefix/mask*

specific-qualifier — Display information about the specified qualifier.

Values port-id, lag-id, host-ip-addr, route-prefix/mask

Output **VRRP Policy Output —** The following table describes the VRRP policy command output fields.

Label	Description
Policy Id	The VRRP priority control policy associated with the VRRP virtual router instance. A value of 0 indicates that no control policy policy is associated with the virtual router instance.
Current Priority & Effects	
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.

Label	Description (Continued)
`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. If the delta-in-use-limit is 0, the sum of the delta priority control events to reduce the virtual router's in-use-priority to 0 can prevent it from becoming or staying master.
`Current Priority`	The configured delta-in-use-limit priority for a VRRP priority control policy or the configured delta or explicit priority for a priority control event.
`Applied`	The number of virtual router instances to which the policy has been applied. The policy cannot be deleted unless this value is 0.
`Description`	A text string which describes the VRRP policy.
`Event Type & ID`	A delta priority event is 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. An explicit priority event is 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 Oper State`	The operational state of the event.
`Hold Set Remaining`	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.
`Priority & Effect`	`Delta` — The *priority-level* value is subtracted from the associated virtual router instance's base priority 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.

Label	Description (Continued)
	`Explicit` — 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.
`In Use`	Specifies whether or not the event is currently affecting the in-use priority of some virtual router.

Sample Output

```
A:ALA-A# show vrrp policy
===============================================================================
VRRP Policies
===============================================================================
Policy    Current             Current      Current      Delta       Applied
Id        Priority & Effect   Explicit     Delta Sum    Limit
-------------------------------------------------------------------------------
1         None                None         None         1           Yes
2         None                None         None         1           No
===============================================================================
A:ALA-A#
```

```
A:ALA-A# show vrrp policy 1
===============================================================================
VRRP Policy 1
===============================================================================
Description     : 10.10.200.253 reachability
Current Priority: None                Applied           : No
Current Explicit: None                Current Delta Sum : None
Delta Limit     : 1

-------------------------------------------------------------------------------
Applied To                      VR     Opr     Base    In-use  Master  Is
Interface Name                  Id             Pri     Pri     Pri     Master
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
Priority Control Events
-------------------------------------------------------------------------------
Event Type & ID                 Event Oper State        Hold Set  Priority In
                                                        Remaining &Effect  Use
-------------------------------------------------------------------------------
Host Unreach 10.10.200.252      n/a                     Expired    20 Del  No
Host Unreach 10.10.200.253      n/a                     Expired    10 Del  No
Route Unknown 10.10.100.0/24    n/a                     Expired     1 Exp  No
===============================================================================
A:ALA-A#
```

VRRP Policy Event Output — The following table describes a specific event VRRP policy command output fields.

Label	Description
`Description`	A text string which describes the VRRP policy.
`Policy Id`	The VRRP priority control policy associated with the VRRP virtual router instance. A value of 0 indicates that no control policy is associated with the virtual router instance.
`Current Priority`	The base router priority for the virtual router instance used in the master election process.
`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.
`Applied`	The number of virtual router instances to which the policy has been applied. The policy cannot be deleted unless this value is 0.
`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. If the delta-in-use-limit is 0, the sum of the delta priority control events to reduce the virtual router's in-use-priority to 0 can prevent it from becoming or staying master.
`Applied to Interface Name`	The interface name where the VRRP policy is applied.
`VR ID`	The virtual router ID for the IP interface.
`Opr`	`Up` — Indicates that the operational state of the VRRP instance is up. `Down` — Indicates that the operational state of the VRRP instance is down.
`Base Pri`	The base priority used by the virtual router instance.
`InUse Priority`	The current in-use priority associated with the VRRP virtual router instance.

Label	Description (Continued)
`Master Priority`	The priority of the virtual router instance which is the current master.
`Priority`	The base priority used by the virtual router instance.
`Priority Effect`	`Delta` — A delta priority event is 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.
`Current Priority`	The configured delta-in-use-limit priority for a VRRP priority control policy or the configured delta or explicit priority for a priority control event.
`Event Oper State`	The operational state of the event.
`Hold Set Remaining`	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.
`Priority`	The base priority used by the virtual router instance.
`Priority Effect`	`Delta` — The *priority-level* value is subtracted from the associated virtual router instance's base priority 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. `Explicit` — 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.
`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.
`Value In Use`	`Yes` — The event is currently affecting the in-use priority of some virtual router.

Label	Description (Continued)
	No — The event is not affecting the in-use priority of some virtual router.
# trans to Set	The number of times the event has transitioned to one of the 'set' states.
Last Transition	The time and date when the operational state of the event last changed.

Sample Output

```
A:ALA-A#show vrrp policy 1 event port-down
===============================================================================
VRRP Policy 1, Event Port Down 1/1/1
===============================================================================
Description     :
Current Priority: None                  Applied           : Yes
Current Explicit: None                  Current Delta Sum : None
Delta Limit     : 1

-------------------------------------------------------------------------------
Applied To                       VR     Opr     Base    In-use  Master  Is
Interface Name                   Id             Pri     Pri     Pri     Master
-------------------------------------------------------------------------------
ies301backup                     1      Down    100     100     0       No

-------------------------------------------------------------------------------
Priority Control Event Port Down 1/1/1
-------------------------------------------------------------------------------
Priority        : 30                    Priority Effect   : Delta
Hold Set Config : 0 sec                 Hold Set Remaining: Expired
Value In Use    : No                    Current State     : Cleared
# trans to Set  : 6                     Previous State    : Set-down
Last Transition : 04/13/2007 04:54:35
===============================================================================
A:ALA-A#

A:ALA-A# show vrrp policy 1 event host-unreachable
===============================================================================
VRRP Policy 1, Event Host Unreachable 10.10.200.252
===============================================================================
Description     : 10.10.200.253 reachability
Current Priority: None                  Applied           : No
Current Explicit: None                  Current Delta Sum : None
Delta Limit     : 1

-------------------------------------------------------------------------------
Applied To                       VR     Opr     Base    In-use  Master  Is
Interface Name                   Id             Pri     Pri     Pri     Master
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
Priority Control Event Host Unreachable 10.10.200.252
-------------------------------------------------------------------------------
Priority        : 20                    Priority Effect   : Delta
Interval        : 1 sec                 Timeout           : 1 sec
Drop Count      : 3
Hold Set Config : 0 sec                 Hold Set Remaining: Expired
```

```
Value In Use    : No                   Current State     : n/a
# trans to Set  : 0                    Previous State    : n/a
Last Transition : 04/13/2007 23:10:24
===============================================================================
A:ALA-A#


A:ALA-A# show vrrp policy 1 event route-unknown
===============================================================================
VRRP Policy 1, Event Route Unknown 10.10.100.0/24
===============================================================================
Description     : 10.10.200.253 reachability
Current Priority: None                 Applied           : No
Current Explicit: None                 Current Delta Sum : None
Delta Limit     : 1

-------------------------------------------------------------------------------
Applied To                      VR     Opr     Base    In-use  Master  Is
Interface Name                  Id             Pri     Pri     Pri     Master
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
Priority Control Event Route Unknown 10.10.100.0/24
-------------------------------------------------------------------------------
Priority        : 1                    Priority Effect   : Explicit
Less Specific   : No                   Default Allowed   : No
Next Hop(s)     : None
Protocol(s)     : None
Hold Set Config : 0 sec                Hold Set Remaining: Expired
Value In Use    : No                   Current State     : n/a
# trans to Set  : 0                    Previous State    : n/a
Last Transition : 04/13/2007 23:10:24
===============================================================================
A:ALA-A#
```

statistics

Syntax **statistics**

Context show>router>vrrp

Description This command displays statistics for VRRP instance.

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

Table 6: Show VRRP Statistics Output

Label	Description
`VR Id Errors`	Displays the number of virtual router ID errors.
`Version Errors`	Displays the number of version errors.
`Checksum Errors`	Displays the number of checksum errors.

Sample Output

```
A:ALA-48# show router vrrp statistics
===============================================================================
VRRP Global Statistics
===============================================================================
VR Id Errors       : 0                  Version Errors     : 0
Checksum Errors    : 0
===============================================================================
A:ALA-48#
```

Monitor Commands

instance

Syntax **instance interface** *interface-name* **vr-id** *virtual-router-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor>router>vrrp

Description Monitor statistics for a VRRP instance.

Parameters *interface-name* — The name of the existing IP interface on which VRRP is configured.

vr-id *virtual-router-id* **—** The virtual router ID for the existing IP interface, expressed as a decimal integer.

interval *seconds* **—** Configures the interval for each display in seconds.

Default 5 seconds

Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

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

rate — When the **rate** keyword is specified, the rate-per-second for each statistic is displayed instead of the delta.

Sample Output

```
*A:ALA-A# monitor router vrrp instance interface n2 vr-id 1
===============================================================================
Monitor statistics for VRRP Instance 1 on interface "n2"
===============================================================================
-------------------------------------------------------------------------------
At time t = 0 sec (Base Statistics)
-------------------------------------------------------------------------------
Become Master       : 1                 Master Changes    : 1
Adv Sent            : 1439              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
===============================================================================
*A:ALA-A#
```

Clear Commands

interface

Syntax **interface** *ip-int-name* [**vrid** *virtual-router-id*]

Context clear>router>vrrp

Description This command resets VRRP protocol instances on an IP interface.

Parameters *ip-int-name* — The IP interface to reset the VRRP protocol instances.

vrid *vrid* — Resets the VRRP protocol instance for the specified VRID on the IP interface.

Default All VRIDs on the IP interface.

Values 1 — 255

statistics

Syntax **statistics** [**policy** *policy-id*]

Context clear>router>vrrp

Description This command enables the context to clear and reset VRRP entities.

Parameters **policy** *policy-id* — Clears statistics for the specified policy.

Values 1 — 9999

statistics

Syntax **statistics interface** *interface-name* [**vrid** *virtual-router-id*]
statistics

Context clear>router>vrrp

Description This command clears statistics for VRRP instances on an IP interface or VRRP priority control policies.

Parameters **interface** *ip-int-name* — Clears the VRRP statistics for all VRRP instances on the specified IP interface.

vrid *virtual-router-id* — Clears the VRRP statistics for the specified VRRP instance on the IP interface.

Default All VRRP instances on the IP interface.

Values 1 — 255

policy [*vrrp-policy-id*] **—** Clears VRRP statistics for all or the specified VRRP priority control policy.

Default All VRRP policies.

Values 1 — 9999

VRRP Debug Commands

events

Syntax
events
events interface *ip-int-name* [**vrid** *virtual-router-id*]
no events
no events interface *ip-int-name* [**vrid** *virtual-router-id*]

Context debug>router>vrrp

Description This command enables debugging for VRRP events.

The **no** form of the command disables debugging.

Parameters *ip-int-name* — Displays the specified interface name.

vrid *virtual-router-id* **—** Displays the specified VRID.

packets

Syntax
packets interface *ip-int-name* [**vrid** *virtual-router-id*]
packets
no packets interface *ip-int-name* [**vrid** *virtual-router-id*] **no packets**

Context debug>router>vrrp

Description This command enables debugging for VRRP packets.

The **no** form of the command disables debugging.

Parameters *ip-int-name* — Displays the specified interface name.

vrid *virtual-router-id* **—** Displays the specified VRID.

Filter Policies

In This Chapter

This chapter provides information about filter policies and management.

Topics in this chapter include:

Filter Policy Configuration Overview

Filter policies, also referred to as Access Control Lists (ACLs), are templates applied to services or network IP interfaces to control network traffic into (ingress) or out of (egress) a service access port (SAP) or network IP interface based on IP and MAC matching criteria. Filters are applied to services to look at packets entering or leaving a SAP . Filters can be used on several interfaces. The same filter can be applied to ingress traffic, egress traffic, or both. Ingress filters affect only inbound traffic destined for the routing complex, and egress filters affect only outbound traffic sent from the routing complex.

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

The available ingress and egress CAM hardware resources can be allocated as per user needs for use with different filter criteria. By default, the system allocates resources to maintain backward compatibility with release 4.0. Users can modify the resource allocation based on their need to scale the number of entries or number of associations (that is, number of SAP/IP interfaces using a filter policy that defines particular match criteria). If no CAM resources are allocated to particular match criteria defined in a filter policy, then the association of that filter policy to a SAP will fail. This is true for both ingress and egress filter policy. Please read the configuration notes section below for more information.

Only one ingress IP or MAC filter policy and one egress IP or MAC filter policy can be applied to a Layer 2 SAP. Both IPv4 and IPv6 ingress and egress filter policy can be used simultaneously with a Layer 2 SAP. Only one ingress IP filter policy and one egress IP filter policy can be applied to a network IP interface. Both IPv4 and IPv6 ingress and egress filter policy can be used simultaneously with an IP interface (For example: network Port IP interface in network mode and IES IP interface in access-uplink mode) for which IPv6 addressing is supported. Network filter policies control the forwarding and dropping of packets based on IP match criteria. Note that non-IP packets are not hitting the IP filter policy, so the default action in the filter policy will not apply to these packets.

Note that non-IP packets are not hitting the IP filter policy, so the default action in the filter policy will not apply to these packets.

Service and Network IP 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.

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

Filter Policy Entities

A filter policy compares the match criteria specified within a filter entry to packets coming through 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, then system executes the default action specified in the filter policy. Each filter policy is assigned a unique filter ID. Each filter policy is defined with:

- Scope
- Default action
- Description

Each filter entry contains:

- Match criteria
- An action

Applying Filter Policies

Filter policies can be applied to specific service types:

- Epipe — Both MAC and IP filters are supported on an Epipe SAP.
- IES — Only IP filters are supported on IES SAP
- VPLS — Both MAC and IP filters are supported on a VPLS SAP.

The table below provides more details on use of filter policies.

Table 7: Applying Filter Policies for 7210 SAS-M and 7210 SAS-X (Network Mode)

Service	IP Filter	IPv6 filter	MAC Filter
Network port IP interface	Network port IP interface (ingress and egress)	Network Port IP interface (ingress and egress)	Not Available
Epipe	Epipe SAP (ingress and egress)	Epipe SAP (ingress and egress)	Epipe SAP (ingress and egress)
VPLS	VPLS SAP (ingress and egress)	VPLS SAP (ingress and egress)	VPLS SAP (ingress and egress)

Table 7: Applying Filter Policies for 7210 SAS-M and 7210 SAS-X (Network Mode)

IES	IES interface SAP (ingress and egress)	Not Available	Not Available
VPRN	VPRN interface SAP (ingress and egress)	Not Available	Not Available
PBB	Ingress and Egress of Epipe I-SAP and I-VPLS I-SAP	Ingress and Egress of Epipe I-SAP, I-VPLS I-SAP and B-VPLS	Ingress and Egress of Epipe I-SAP, I-VPLS I-SAP and B-VPLS

Table 8: Applying Filter Policies for 7210 SAS-M (Access-uplink mode)

Service	IP Filter	IPv6 filter	MAC Filter	Mode (For 7210 SAS-M devices only)
Epipe	Epipe access SAP (egress and ingress), Epipe access-uplink SAP (egress and ingress)	Epipe (egress and ingress), Epipe access-uplink SAP (egress and ingress)	Epipe (egress and ingress), Epipe access-uplink SAP (egress and ingress)	Epipe
VPLS	VPLS access SAP (ingress and egress), VPLS access-uplink SAP (ingress and egress)	VPLS access SAP (ingress and egress), VPLS access-uplink SAP (ingress and egress)	VPLS access SAP (ingress and egress), VPLS access-uplink SAP (ingress and egress)	VPLS
RVPLS (VPLS SAPs)	VPLS access (ingress and egress) and access-uplink SAPs (ingress and egress)	Not Available	Not Available	RVPLS (VPLS SAPs)

Table 8: Applying Filter Policies for 7210 SAS-M (Access-uplink mode)

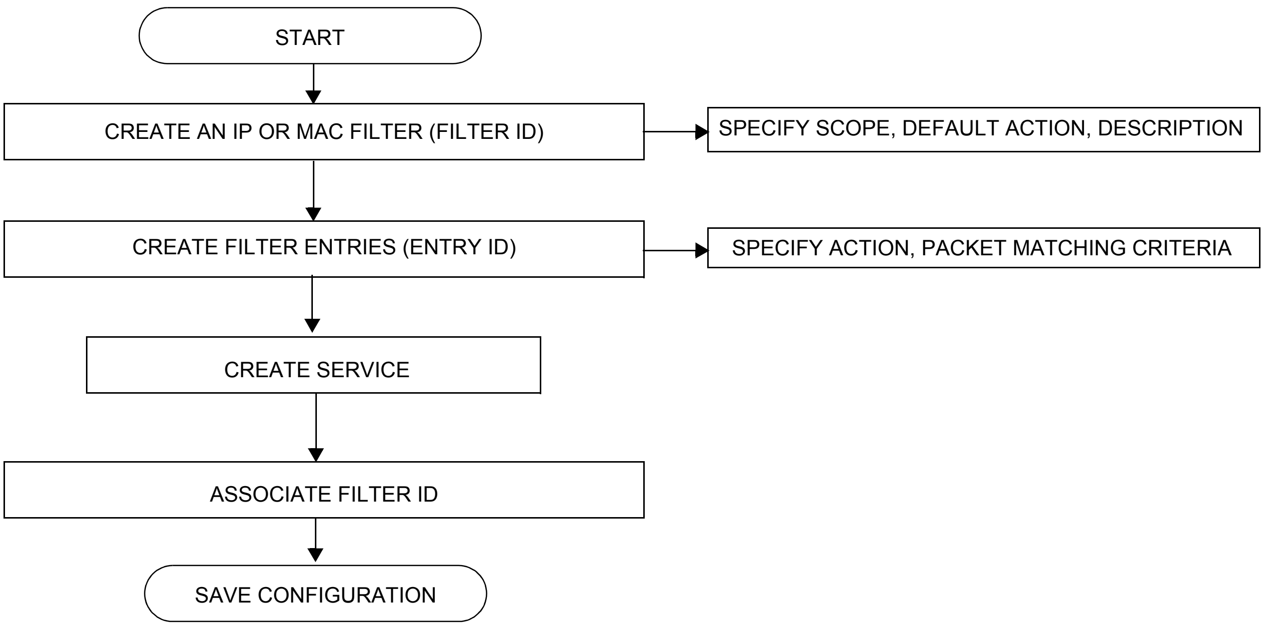
RVPLS (RVPLS IES IP Interface)	Ingress Override filters (ingress)	Not Available	Not Available	VPLS (RVPLS IES IP Interface)
IES	IES access SAP, IES access-uplink SAP	IES access-uplink SAP	Not Available	IES
Epipe	Epipe access SAP (egress and ingress), Epipe access-uplink SAP (egress and ingress)	Epipe (egress and ingress), Epipe access-uplink SAP (egress and ingress)	Epipe (egress and ingress), Epipe access-uplink SAP (egress and ingress)	Epipe

Filter policies are applied to the following service entities:

- SAP ingress — IP and MAC filter policies applied on the SAP ingress define the Service Level Agreement (SLA) enforcement of service packets as they ingress a SAP according to the filter policy match criteria.
- SAP egress — Filter policies applied on SAP egress define the Service Level Agreement (SLA) enforcement for service packets as they egress on the SAP according to the filter policy match criteria.
- (ingress and egress)Network ingress — IP filter policies are applied to network ingress IP interfaces.
- Network egress — IP filter policies are applied to network egress IP interfaces.

Creating and Applying Policies

Figure 6 displays the process to create filter policies and apply them to a service network IP interface.



Packet Matching Criteria

Up to 65535 IP and 65535 MAC filter IDs (unique filter policies) can be defined. A maximum of 16384 filter entries can be defined in one filter at the same time. Each filter ID can contain up to 65535 filter entries. As few or as many match parameters can be specified as required, but all conditions must be met in order for the packet to be considered a match and the specified action performed. The process stops when the first complete match is found and then executes the action defined in the entry, either to drop or forward packets that match the criteria.

IP filter policies match criteria that associate traffic with an ingress or egress SAP. Matching criteria to drop or forward IP traffic include:

- Source IP address and mask

  Source IP address and mask values can be entered as search criteria. The IP Version 4 addressing scheme consists of 32 bits expressed in dotted decimal notation (X.X.X.X).

  Address ranges are configured by specifying mask values, the 32-bit combination used to describe the address portion which refers to the subnet and which portion refers to the host. The mask length is expressed as an integer (range 1 to 32).

  The IP Version 6 (IPv6) addressing scheme consists of 128 bits expressed in compressed representation of IPv6 addresses (RFC 1924, *A Compact Representation of IPv6 Addresses*). 7210 supports use of either IPv6 64-bit address match or IPv6 128-bit address match. Use of IPv6 64-bit address in the match criteria provides better scale but provides lesser IPv6 header fields for match criteria. Use of IPv6 128-bit address in the match criteria provides lesser scale but provides more IPv6 header fields for match criteria.
- Destination IP address and mask — Destination IP address and mask values can be entered as search criteria. Similar choice as available for source IPv6 addresses is available for destination IPv6 addresses (see above).
- Protocol — Entering a protocol ID (such as TCP, UDP, etc.) allows the filter to search for the protocol specified in this field.
- Protocol — For IPv6: entering a next header allows the filter to match the first next header following the IPv6 header.
- Source port — Entering the source port number allows the filter to search for matching TCP or UDP port values.
- Destination port — Entering the destination port number allows the filter to search for matching TCP or UDP port.
- DSCP marking — Entering a DSCP marking enables the filter to search for the DSCP marking specified in this field. See Table 11, DSCP Name to DSCP Value Table, on page 223.
- ICMP code — Entering an ICMP code allows the filter to search for matching ICMP code in the ICMP header.

- ICMP type — Entering an ICMP type allows the filter to search for matching ICMP types in the ICMP header.
- Ipv4 filter created in the mode to use ipv6 resource cannot be applied at egress SAP. Similarly IPv4 filter created in the mode to use IPv6 resource, will fail to match fragment option.
- Fragmentation — IPv4 only: Enable fragmentation matching. A match occurs if packets have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value.
- Option present — Enabling the option presence allows the filter to search for presence or absence of IP options in the packet. Padding and EOOL are also considered as IP options.
- TCP-ACK/SYN flags — Entering a TCP-SYN/TCP-ACK flag allows the filter to search for the TCP flags specified in these fields.

MAC filter policies match criteria that associate traffic with an ingress or egress SAP. Matching criteria to drop or forward MAC traffic include:

- Source MAC address and mask

  Entering the source MAC address range allows the filter to search for matching a source MAC address and/or range. Enter the source MAC address and mask in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx; for example, 00:dc:98:1d:00:00.
- Destination MAC address and mask

  Entering the destination MAC address range allows the filter to search for matching a destination MAC address and/or range. Enter the destination MAC address and mask in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx; for example, 02:dc:98:1d:00:01.
- Dot1p and mask

  Entering an IEEE 802.1p value or range allows the filter to search for matching 802.1p frame. The Dot1p and mask accepts decimal, hex, or binary in the range of 0 to 7.
- Ethertype

  Entering an Ethernet type II Ethertype value to be used as a filter match criterion. The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. The Ethertype accepts decimal, hex, or binary in the range of 1536 to 65535.

  Note that the 7210 SAS M does not support frame-type “EthernetII” but ether-type is supported as a match field. By default the frame-type is set to “EthernetII in the 7210 SAS M, as compared to 803dot3 in the 7x50. This allows the ether-type to be configured as a match field without configuring the frame-type as ethernetII.

DSCP Values

Table 11: DSCP Name to DSCP Value Table

DSCP Name	Decimal DSCP Value	Hexadecimal DSCP Value	Binary DSCP Value
default	0	*	
cp1	1		
cp2	2		
cp3	3		
cp4	4		
cp5	5		
cp6	6		
cp7	7	*	
cs1	8		
cp9	9		
af11	11	*	
af12	12	*	
cp13	13		
cp15	15		
cs2	16	*	
cp17	17		
af21	18	*	
cp19	19		
af22	20	*	
cp21	21		
af23	22	*	
cp23	23		
cs3	24	*	
cp25	25		
af31	26	*	
cp27	27		
af32	28	*	
cp29	29		
af33	30	*	
cp21	31		

Table 11: DSCP Name to DSCP Value Table (Continued)

DSCP Name	Decimal DSCP Value	Hexadecimal DSCP Value	Binary DSCP Value
cs4	32	*	
cp33	33		
af41	34	*	
cp35	35		
af42	36	*	
cp37	37		
af43	38	*	
cp39	39		
cs5	40	*	
cp41	41		
cp42	42		
cp43	43		
cp44	44		
cp45	45		
ef	46	*	
cp47	47		
nc1	48	*	(cs6)
cp49	49		
cp50	50		
cp51	51		
cp52	52		
cp53	53		
cp54	54		
cp55	55		
cp56	56		
cp57	57		
nc2	58	*	(cs7)
cp60	60		
cp61	61		
cp62	62		

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. 7210 SAS supports either drop or forward action.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 an ascending entry ID order. To reorder entries in a filter policy, edit the entry ID value; for example, to reposition entry ID 6 to a more explicit location, change the entry ID *6* value to entry ID *2*.

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

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

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

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

Figure 5 displays an example of several packets forwarded upon matching the filter criteria and several packets traversing through the filter entries and then dropped.

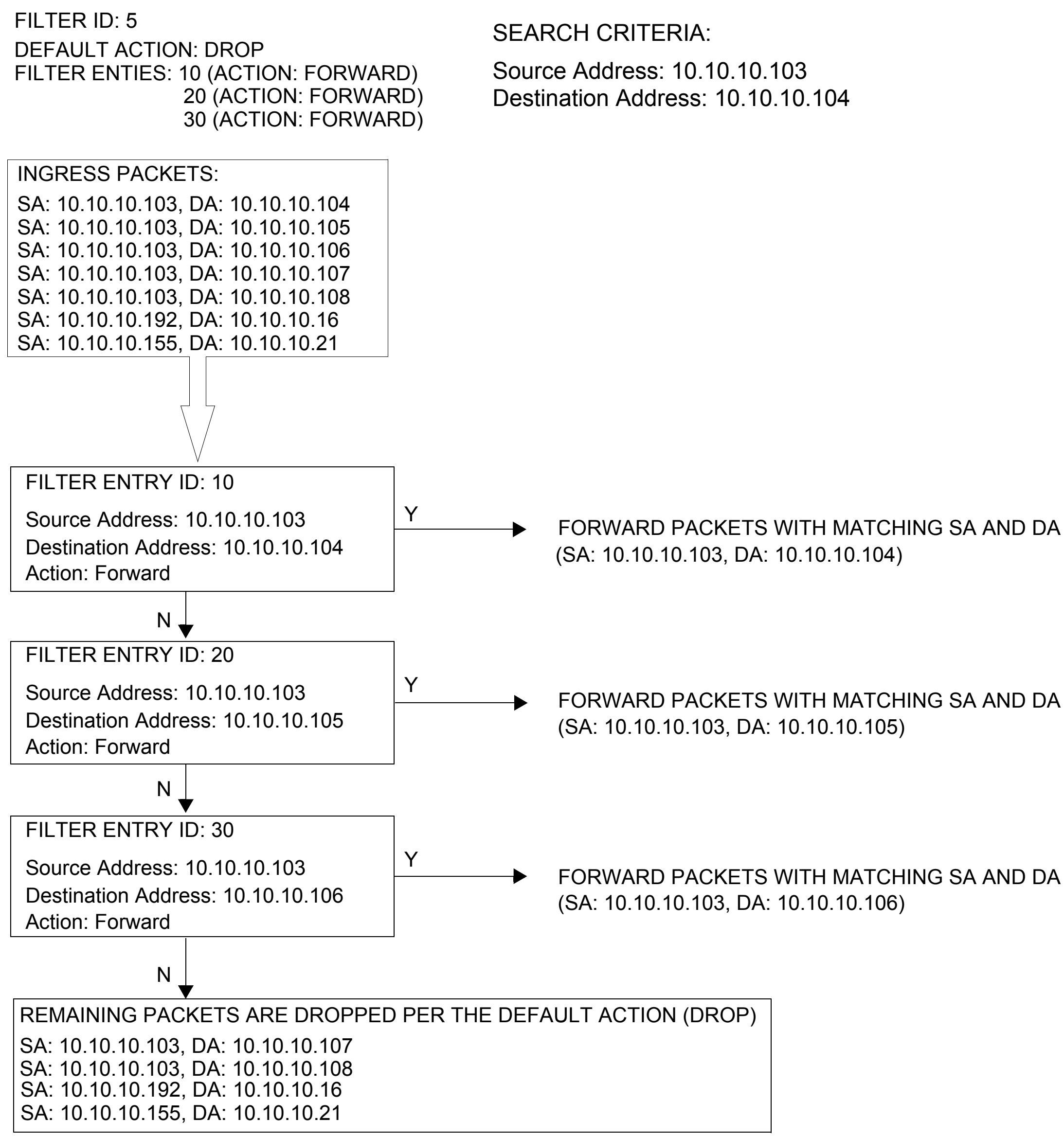


Figure 5: Filtering Process Example

Applying Filters

After filters are created, they can be applied to the following entities:

- Applying a Filter to a SAP on page 227
- Applying a Filter to a Network IP Interface on page 227

Applying a Filter to a SAP

During the SAP creation process, ingress and egress filters are selected from a list of qualifying IP and MAC filters. When ingress filters are applied to a SAP, packets received at the SAP are checked against the matching criteria in the filter entries. If the packet completely matches all criteria in an entry, the checking stops and an entry action is performed. If permitted, the traffic is forwarded according to the specification of the action. If the packets do not match, the default filter action is applied. If permitted, the traffic is forwarded.

When egress filters are applied to a SAP, packets received at the egress SAP are checked against the matching criteria in the filter entries. If the packet completely matches all criteria in an entry, the checking stops. If permitted, the traffic is transmitted. If denied, the traffic is dropped. If the packets do not match, the default filter action is applied.

Filters can be added or changed to an existing SAP configuration by modifying the SAP parameters. Filter policies are not operational until they are applied to a SAP and the service enabled.

Applying a Filter to a Network IP Interface

An IP filter can be applied to a network portIP interface. Packets received on the interface are checked against the matching criteria in the filter entries. If the packet completely matches all criteria in an entry, the checking stops. If permitted, the traffic is forwarded. If the packets do not match, they are discarded or forwarded based on the default action specified in the policy.

Configuration Notes

NOTE: Please refer to the 7210 Services Guides for Service specific ACL support and restrictions.

The following information describes filter implementation caveats:

- Creating a filter policy is optional.
- Associating a service with a filter policy is optional.
- When a filter policy is configured, it should be defined as having either an *exclusive* scope for one-time use, or a *template* scope meaning that the filter can be applied to multiple SAPs.
- A specific filter must be explicitly associated with a specific service in order for packets to be matched.
- A filter policy can consist of zero or more filter entry. Each entry represents a collection of filter match criteria. When packets enter the ingress or egress ports, packets are compared to the criteria specified within the entry or entries.
- When a large (complex) filter is configured, it may take a few seconds to load the filter policy configuration and be instantiated.
- The action keyword must be entered for the entry to be active. Any filter entry without the action keyword will be considered incomplete and be inactive.
- If the command **config>system>resource-profile> g8032-fast-flood-enable** is enabled, the resources are shared with G.8032 Ethernet rings. For more information refer to 7210 SAS M,X OS Interface Configuration guide. Additionally refer to the 7210 Basic Systems Guide for more information about resource allocation to different features.
- When a filter policy is created with the option ipv6-64bit-address, the entries can only use only the IPv6 src-ip and IPv6 dst-ip fields in the match criteria.
- When a filter policy is created with the option ipv6-128bit-address, the entries can use the IPv6 src-ip, IPv6 dst-ip, IPv6 DSCP, TCP/UDP port numbers (source and destination port), ICMP code and type, and TCP flags fields in the match criteria.
- The resources must be allocated for use by ingress IPv6 filters, before associating an IPv6 filter policy to a SAP. By default, the software does not enable the use of IPv6 resources. Until resources are allocated for use by IPv6 filters, software fails all attempts to associate a IPv6 filter policy with a SAP.
- The available ingress CAM hardware resources can be allocated as per user needs for use with different filter criteria using the commands under configure> system> resource-profile> ingress-internal-tcam> acl-sap-ingress. By default, the system allocates resources to maintain backward compatibility with release 4.0. Users can modify the resource allocation based on their need to scale the number of entries or number of associations (that is, number of SAP/IP interfaces using a filter policy that defines a particular match criterion).The available egress CAM hardware resources can be allocated as per user needs for use with different filter criteria using the commands under configure>

system>resource-profile> egress-internal-tcam> acl-sap-egress. By default, the system allocates resources to maintain backward compatibility with release 4.0. Users can modify the resource allocation based on their needs to scale the number of entries or the number of associations (that is, number of SAP/IP interfaces using a filter policy that defines a particular match criterion).

- IPv6 ACLs and MAC QoS policies cannot co-exist on the SAP.
- If no CAM resources are allocated to a particular match criterion defined in a filter policy, then the association of that filter policy to a SAP will fail. This is true for both ingress and egress filter policy.
- IPv6 ACLs and MAC QoS policies cannot co-exist on the SAP.
- For traffic ingressing a B-VPLS SAP and destined to a B-VPLS SAP, the MAC filter matches the B-domain, MAC header fileds (that is, B-DA, B-SA, and others). The MAC filter can be used to match customer payload MAC header fields for traffic ingressing a B-VPLS SAP and destined to an I-VPLS SAP.

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 VPLS or IES services.
- Some of the MAC match criteria fields are exclusive to each other, based on the type of Ethernet frame. Use the following table to determine the exclusivity of fields.In the 7210 SAS, the default frame-format is “EthernetII”

Table 12: MAC Match Criteria Exclusivity Rules

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

IP Filters

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

IPv6 Filters

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

Resource Usage for Ingress Filter Policies

When the user allocates resources from the ingress CAM resource pool for use by filter policies using the configure> system> resource-profile CLI commands, the system allocates resources in chunks of 256 entries. The usage of these entries by different type of match criteria is given below:

- **mac-criteria** - User needs to allocate resources for mac-criteria from the filter resource pool by using the command “configure> system> resource-profile> ingress-internal-tcam>acl-sap-ingress> mac-match-enable" before using ingress ACLs with mac-criteria. Every entry configured in the filter policy using the mac-criteria uses one (1) entry from the chunks allocated for use by mac-criteria in the hardware. For example: Assume a filter policy is configured with 50 entries and uses “configure>system> resource-profile> ingress-internal-tcam> acl-sap-ingress> mac-match-enable 1”, the user configures one chunk for use by mac-criteria (allowing a total of 256 entries. one reserved for internal use entries for use by SAPs using filter policies that use mac-criteria). In this case, the user can have 5 SAPs using mac-criteria filter policy and consumes 250 entries.
- **ipv4-criteria** - User needs to allocate resources for ip(v4)-criteria from the filter resource pool by using the command "configure> system> resource-profile> ingress-internal-tcam> acl-sap-ingress> ipv4-match-enable" before using ingress ACLs with ipv4-criteria. The resource usage per IPv4 match entry is same as the mac-criteria. Please check the above example. When created with "use-ipv6-resource" the resource usage is the same as IPv6 filters using ipv6-128-bit-addresses.

- **ipv6-criteria using ipv6-64-bit addresses** - User needs to allocate resources for ipv6-criteria with 64-bit address match from the filter resource pool by using the command "configure> system> resource-profile> ingress-internal-tcam> acl-sap-ingress> ipv6-64only-match-enable" before using ingress ACLs with ipv6-criteria that use only IPv6 64-bit address for source and destination IPv6 addresses. The IPv6 headers fields available for match is limited. Please see the CLI description for filter below for more information. The usage is same as the ipv4 and mac-criteria.
- **ipv6-criteria using ipv6-128-bit addresses** - User needs to allocate resources for ipv6-criteria with 128-bit address match from the filter resource pool by using the command "configure> system> resource-profile> ingress-internal-tcam> acl-sap-ingress> ipv4-ipv6-128-match-enable" before using ingress ACLs with ipv6-criteria that use only IPv6 128-bit address for source and destination IPv6 addresses. These resources can be shared by a policy that uses only IPv4 criteria entries. Every entry configured in the filter policy using the ipv6-criteria with 128-bit addresses uses two (2) entries from the chunks allocated for use by ipv6-criteria (128-bit) in the hardware. For example: Assume a filter policy is configured with 50 entries and using “configure>system> resource-profile> ingress-internal-tcam> acl-sap-ingress> ipv4-ipv6-128-match-enable 1”, the user configures one chunk for use by ipv6-criteria with 128-bit addresses (allowing for a total of 128 entries for use by SAPs using filter policies that use this criteria). In this case, user can have five (5) SAPs using this filter policy and consumes 125 entries. Note when a chunk is allocated to IPv6 criteria, software automatically adjusts the number of available entries in that chunk to 128, instead of 256, since 2 entries are needed to match IPv6 fields.

The users can use “tools>dump> system-resources” command to know the current usage and availability. For example: Though chunks are allocated in 256 entries, only 128 entries show up against filters using those of IPv6 128-bit addresses. One or more entries are reserved for system use and is not available for user.

Resource Usage for Egress Filter Policies

7210 SAS-E does not support allocation of egress CAM resources and these resources are pre-allocated on boot up by software.

When the user allocates resources for use by filter policies using the *configure> system> resource-profile> egress-internal-tcam>* CLI commands, the system allocates resources in chunks of 512 entries from the egress internal tcam pool in hardware. The usage of these entries by different type of match criteria is given below:

- **mac-criteria** - The user needs to allocate resources for using mac-criteria using the command “*configure> system> resource-profile> egress-internal-tcam> acl-sap-egress> mac-match-enable 2*” or “*configure> system> resource-profile> egress-internal-tcam> acl-sap-egress> mac-ipv4-match-enable 2*” or “*configure> system> resource-profile> egress-internal-tcam> acl-sap-egress> mac-ipv6-64bit-match-enable 2*”. In the last two cases, the resources can be shared with SAPs that use IPv4 or IPv6 64-bit filter policies.

The first case allocates resources for exclusive use by MAC filter policies. The resource usage varies based how resources have been allocated:

- If resources are allocated for use by mac-criteria only (using mac-match-enable), then every entry configured in the filter policy uses one (1) entry from the chunks allocated for use by mac-criteria in the hardware. **For example:** Assume a filter policy is configured with 25 mac-criteria entries and uses "*configure> system> resource-profile> egress-internal-tcam> acl-sap-egress> mac-match-enable 2*", the user configures two chunks for use by mac-criteria, allowing a total of 512 entries for use by SAPs using filter policies that use mac-criteria. Therefore, the user can have about 10 SAPs using mac-criteria filter policy and consumes 500 entries. With this, SAPs using ipv4 criteria or ipv6 criteria cannot share the resources along with SAPs using mac-criteria.
- If the resources are allocated for sharing between mac-criteria and ipv4-criteria, then every entry configured in the filter policy uses 2 (two) entries from the chunks allocated in hardware. **For example:** Assume a filter policy is configured with 25 mac-criteria entries and another filter policy configured with 25 IPv4 criteria entries and, with mac-ipv4-match-enable set to 2, that is, user configures two chunks for sharing between MAC and IPv4, allowing for a total of entries for use by SAPs that use filter policies using ipv4-criteria or mac-criteria. Therefore, the user can have about 4 SAPs using filter policies, such that 2 SAPs uses mac-criteria and the other 2 SAPs use ipv4-criteria or any combination thereof.
- If the resources are allocated for sharing between mac-criteria and ipv6-64bit-criteria, then every entry configured in the filter policy uses 2 (two) entries from the chunks allocated in hardware. **For example:** Assume a filter policy is configured with 50 mac-criteria entries and another filter policy configured with 50 IPv6 64-bit criteria entries and, with mac-ipv6-64bit-match-enable set to 2, that is, user configures two chunks for sharing between MAC and IPv6-64bit, allowing for a total of 128 entries for use by SAPs that use filter policies using ipv6-64bit-criteria or mac-criteria. Therefore, the user can have about 2 SAPs using filter policies, such that one SAP uses mac-criteria and the other one SAP uses ipv6-64bit-criteria or any combination thereof.

• **ipv4-criteria** - The user need to allocate resources using the command *"configure> system> resource-profile> egress-internal-tcam> acl-sap-egress> mac-ipv4-match-enable*". The resource usage is as explained above.

• **ipv6-criteria using ipv6-64-bit addresses** - The user need to allocate resources using the command "*configure> system> resource-profile> egress-internal-tcam> acl-sap-egress> mac-ipv6-64bit-match-enable*". The resource usage is as explained above.

• **ipv6-criteria using ipv6-128-bit addresses -** The user need to allocate resources using the command "*configure> system> resource-profile> egress-internal-tcam> acl-sap-egress> ipv6-128bit-match-enable*". This command allocates resources for exclusive by IPv6-128bit criteria filter policies and cannot be shared by SAPs using any another criteria. If resources are allocated for use by ipv6-128bit-criteria only, then every entry configured in the filter policy uses two (2) entries from the chunks allocated for use in hardware. **For**

example: Assume a filter policy is configured with 50 ipv6-128bit-criteria entries and user uses “*configure> system> resource-profile> egress-internal-tcam> acl-sap-egress> ipv6-128bit-match-enable 2*”, to configure two chunks for use by ipv6-128bit-criteria. This allows for a total of 128 for use by SAPs using filter policies that use ipv6-128bit-criteria. Therefore the user can have about 2 SAPs using ipv6-128bit-criteria filter policy and consumes 100 entries.

The user can use “tools>dump> system-resources” command to know the current usage and availability.

Configuring Filter Policies with CLI

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

Topics in this section include:

Basic Configuration

The most basic IP and MAC filter policies must have the following:

- A filter ID
- Template scope, either *exclusive* or *template*
- Default action, either drop or forward
- At least one filter entry
  - → Specified action, either drop or forward
  - → Specified matching criteria
- Allocates the required amount of resources for ingress and egress filter policies

The following example displays a sample configuration of allocation of ingress internal CAM resources for ingress policy for 7210 SAS-M:

```
*A:7210SAS>config>system>res-prof>ing-internal-tcam>acl-sap-ing# info detail

----------------------------------------------
                    ipv4-match-enable max
                    ipv6-64-only-match-enable 1
                    no ipv4-ipv6-128-match-enable
----------------------------------------------

*A:7210SAS>config>system>res-prof>ing-internal-tcam>acl-sap-ing# back
```

The following example displays a sample configuration of allocation of egress internal CAM resources for egress policy for 7210 SAS-M and SASX:

```
A:7210SAS>config>system>res-prof>egr-internal-tcam# info detail
----------------------------------------------
                acl-sap-egress 2
                    mac-ipv4-match-enable 2
                    ipv6-128bit-match-enable 0
                    mac-ipv6-64bit-match-enable 0
                    mac-match-enable 0
                exit
----------------------------------------------
*A:7210SAS>config>system>res-prof>egr-internal-tcam# acl-sap-egress
```

The following example displays a sample configuration of an IP filter policy. The configuration blocks all incoming TCP session except Telnet and allows all outgoing TCP sessions from IP net 10.67.132.0/24. CAM resources must be allocated to IPv4 criteria before associating the filter with a SAP. Figure 6 depicts the interface to apply the filter.

```
A:ALA-1>config>filter# info
----------------------------------------------
        ip-filter 3 create
```

```
            entry 10 create
                match protocol 6
                    dst-port eq 23
                    src-ip 10.67.132.0/24
                exit
                action forward
            exit
            entry 20 create
                match protocol 6
                    tcp-syn true
                    tcp-ack false
                exit
                action drop
            exit
        exit
----------------------------------------------
A:ALA-1>config>filter#
```

The following is the configuration example of ingress-internal-tcam in 7210 SAS-X.

```
A:7210SAS>config>system>res-prof>ing-internal-tcam>acl-sap-ing# info detail
----------------------------------------------
ipv4-match-enable max
no ipv6-64-only-match-enable
no ipv4-ipv6-128-match-enable
----------------------------------------------
*A:7210SAS>config>system>res-prof>ing-internal-tcam>acl-sap-ing# ipv6-64-
```

The following figure shows the IP filter applied to an ingress interface.

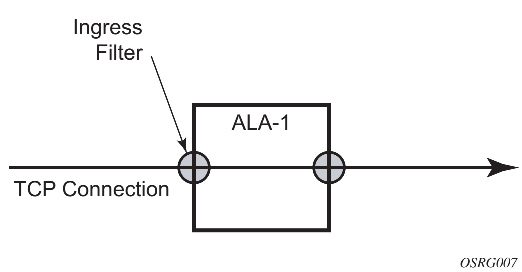


Figure 6: Applying an IP Filter to an Ingress Interface

Common Configuration Tasks

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

To configure a filter policy, perform the following tasks:

- Creating an IP Filter Policy on page 238
- Creating a MAC Filter Policy on page 243
- Filter policies can be associated with the following entities: on page 88
- Apply Filter Policies to a Network IP Interface on page 247

Allocating Resources for Filter policies (Ingress and Egress)

The following provides an example of allocation of CAM hardware resources for use with filter policies that use IPv4 and MAC criteria:

Creating an IP Filter Policy

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

- The filter type specified (IP)
- A filter policy ID
- A default action, either drop or forward
- Filter policy scope specified, either *exclusive* or *template*
- At least one filter entry with matching criteria specified
- Configure CAM hardware resource for use by the filter policy match-criteria

IP Filter Policy

The following displays an exclusive filter policy configuration example:

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

```
----------------------------------------------
A:ALA-7>config>filter#
```

IP Filter Entry

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

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

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

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

The following displays an IP filter entry configuration example.

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

IP Entry Matching Criteria

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

The following displays an IP filter matching configuration.

```
*A:ALA-48>config>filter>ip-filter# info
----------------------------------------------
            description "filter-mail"
            scope exclusive
            entry 10 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
                action forward
            exit
----------------------------------------------
*A:ALA-48>config>filter>ip-filter#
```

Creating an IPv6 Filter Policy

Configuring and applying IPv6 filter policies is optional. Each filter policy must have the following:

- The IPv6 filter type specified.
- An IPv6 filter policy ID.
- A default action, either drop or forward.
- Template scope specified, either exclusive or template.
- At least one filter entry with matching criteria specified.

IPv6 Filter Policy

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

To create an IPv6 filter using 64-bit-address, the user can use the command “Config> filter> ipv6-filter <filter-id> ipv6-64bit-address create”.

By default, the ipv6 filters are configured using 128-bit-address, the output is as shown below:

```
*A:7210SAS>config>filter>ipv6-filter# info detail
----------------------------------------------
            default-action drop
```

```
            no description
            scope template
            exit
*A:7210SAS>config>filter>ipv6-filter#
```

IPv6 Filter Entry

Within an IPv6 filter policy, configure filter entries which contain criteria against which ingress, egress, or network traffic is matched. The action specified in the entry determine how the packets are handled, either dropped or forwarded.

- Enter an IPv6 filter entry ID. The system does not dynamically assign a value.
- Assign an action, either drop or forward.
- Specify matching criteria.

The following displays an IPv6 filter entry configuration example:

```
*A:7210SAS>config>filter>ipv6-filter# info detail
----------------------------------------------
            default-action drop
            no description
            scope template
            entry 1 create
                no description
                match next-header none
                    no dscp
                    no dst-ip
                    no dst-port
                    src-ip 1::1/128
                    no src-port
                    no tcp-syn
                    no tcp-ack
                    no icmp-type
                    no icmp-code
                exit
                action forward
            exit
*A:7210SAS>config>filter>ipv6-filter#
```

Creating a MAC Filter Policy

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

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

MAC Filter Policy

The following displays an MAC filter policy configuration example:

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

MAC Filter Entry

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

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

The following displays a MAC filter entry configuration example:

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

MAC Entry Matching Criteria

The following displays a filter matching configuration example.

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

Apply IP and MAC Filter Policies

The following example shows an example of applying an IP and a MAC filter policy to an Epipe service:

CLI Syntax:
```
config>service# epipe service-id
  sap sap-id
     egress
        filter {ip ip-filter-id | mac mac-filter-id}
     ingress
        filter {ip ip-filter-id | mac mac-filter-id}
```

The following output displays IP and MAC filters assigned to an ingress and egress SAP:

```
A:ALA-48>config>service>epipe# info
----------------------------------------------
            sap 1/1/1.1.1 create
                ingress
                    filter ip 10
                exit
                egress
                    filter mac 92
                exit
            exit
            no shutdown
----------------------------------------------
A:ALA-48>config>service>epipe#
```

Apply an IPv6 Filter Policy to VPLS

The following output displays an IPv6 filters assigned to VPLS service interface:

```
*A:7210SAS>config>router#vpls# info detail
----------------------------------------------
......
                    ingress
                        counter-mode in-out-profile-count
                        no drop-count-extra-vlan-tag-pkts
                    exit
                exit
                ingress
                    qos 1
                    no aggregate-meter-rate
                    filter ipv6 1
                exit
                egress
                    no filter
                exit
                no collect-stats
                no accounting-policy
                no shutdown
            exit

*A:7210SAS>config>router#vpls 2 info detail
```

Apply Filter Policies to a Network IP Interface

IP filter policies can be applied to network IP interfaces. MAC filters cannot be applied to network IP interfaces or to routable IES services.

Apply an IP Interface

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

The following displays an IP filter applied to an interface at ingress.

```
A:ALA-48>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
...
        interface "to-104"
            address 10.0.0.103/24
            port 1/1/1
            ingress
                filter ip 10
            exit
            egress
                filter ip 10
            exit
        exit
...
#------------------------------------------
A:ALA-48>config>router#
```

Filter Management Tasks

This section discusses the following filter policy management tasks:

- Renumbering Filter Policy Entries on page 248
- Modifying an IP Filter Policy on page 250
- Detaching/Deleting a Filter Policy on page 253
- Copying Filter Policies on page 255

Renumbering Filter Policy Entries

The system 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 renumber existing MAC or IP filter entries to re-sequence filter entries:

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

Example:
```
config>filter>ip-filter# renum 10 15
config>filter>ip-filter# renum 20 10
config>filter>ip-filter# renum 40 1
```

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

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "filter-main"
            scope exclusive
            entry 10 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
                action forward
            exit
            entry 20 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
            entry 30 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.200/24
                exit
                action forward
            exit
            entry 40 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
        exit
...
----------------------------------------------
A:ALA-7>config>filter#
```

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "filter-main"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 10 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
            entry 15 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
                action forward
            exit
            entry 30 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.200/24
                exit
                action forward
            exit
        exit
...
----------------------------------------------
A:ALA-7>config>filter#
```

Modifying an IP Filter Policy

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

Example:

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

The following output displays the modified IP filter output:

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "New IP filter info"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 2 create
                description "new entry"
                match
                    dst-ip 10.10.10.104/32
                exit
                action drop
            exit
            entry 10 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.100/24
                exit
                action drop
            exit
            entry 15 create
                description "no-91"
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.103/24
                exit
                action forward
            exit
            entry 30 create
                match
```

```
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.0.200/24
                exit
                action forward
            exit
        exit
..
----------------------------------------------
A:ALA-7>config>filter#
```

Modifying an IPv6 Filter Policy

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

Example: config>filter# ipv6-filter 11

config>filter>ipv6-filter# description "IPv6 filter for Customer 1"

config>filter>ipv6-filter# scope exclusive

config>filter>ipv6-filter# entry 1

config>filter>ipv6-filter>entry# description "Fwds matching packets"

config>filter>ipv6-filter>entry# action forward

config>filter>ipv6-filter>entry# exit

The following output displays the modified IPv6 filter output:

```
A:7210SAS>config>filter>ipv6-filter# info detail
----------------------------------------------
            default-action drop
            no description
            scope template
            entry 1 create
                description "Test"
                match next-header none
                    no dscp
                    no dst-ip
                    no dst-port
                    src-ip 1::1/128
                    no src-port
                    no tcp-syn
                    no tcp-ack
                    no icmp-type
                    no icmp-code
                exit
                action forward
            exit
...
A:7210SAS>config>filter>ipv6-filter
```

Modifying a MAC Filter Policy

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

Example:
```
config>filter# mac-filter 90
config>filter>mac-filter# description "New filter info"
config>filter>mac-filter# entry 1
config>filter>mac-filter>entry# description "New entry info"
config>filter>mac-filter>entry# action forward
config>filter>mac-filter>entry# exit
config>filter>mac-filter# entry 2 create
config>filter>mac-filter>entry$ action drop
config>filter>mac-filter>entry# match
config>filter>mac-filter>entry>match# dot1p 7 7
```

The following output displays the modified MAC filter output:

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        mac-filter 90 create
            description "New filter info"
            scope exclusive
            entry 1 create
                description "New entry info"
                match
                    src-mac 00:dc:98:1d:00:00 ff:ff:ff:ff:ff:ff
                    dst-mac 02:dc:98:1d:00:01 ff:ff:ff:ff:ff:ff
                exit
                action forward
            exit
            entry 2 create
                match
                    dot1p 7 7
                exit
                action drop
            exit
        exit
...
----------------------------------------------
A:ALA-7>config>filter#
```

Detaching/Deleting a Filter Policy

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

- From an Ingress SAP on page 253
- From an Egress SAP on page 253
- From a Network Interface on page 254
- From the Filter Configuration on page 254

From an Ingress SAP

To remove a filter from an ingress SAP, enter the following CLI commands:

CLI Syntax:
```
config>service# [epipe | vpls] service-id
  sap port-id[:encap-val]
    ingress
          no filter
```

Example:
```
config>service# epipe 5
config>service>epipe# sap 1/1/2:3
config>service>epipe>sap# ingress
config>service>epipe>sap>ingress# no filter
```

From an Egress SAP

To remove a filter from an egress SAP, enter the following CLI commands:

CLI Syntax:
```
config>service# [epipe | vpls] service-id
  sap port-id[:encap-val]
    egress
          no filter
```

Example:
```
config>service# epipe 5
config>service>epipe# sap 1/1/2:3
config>service>epipe>sap# egress
config>service>epipe>sap>egress# no filter
```

From a Network Interface

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

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

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

From the Filter Configuration

After you have removed the filter from the SAP, use the following CLI syntax to delete the filter.

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

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

Example: `config>filter# no ip-filter 11 config>filter# no mac-filter 13`

Copying Filter Policies

When changes are made to an existing filter policy, they are applied immediately to all services where the policy is applied. If numerous changes are required, the policy can be copied so you can edit the "work in progress" version without affecting the filtering process. When the changes are completed, you can overwrite the work in progress version with the original version.

New filter policies can also be created by copying an existing policy and renaming the new filter.

CLI Syntax: `config>filter# copy` *`filter-type src-filter-id`* `[src-entry` *`src-entry-id`*`] to` *`dst-filter-id`* `[dst-entry` *`dst-entry-id`*`] [overwrite]`

The following displays the command usage to copy an existing IP filter (**11**) to create a new filter policy (**12**).

Example: `config>filter# copy ip-filter 11 to 12`

```
A:ALA-7>config>filter# info
----------------------------------------------
...
        ip-filter 11 create
            description "This is new"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 2 create
...
        ip-filter 12 create
            description "This is new"
            scope exclusive
            entry 1 create
                match
                    dst-ip 10.10.10.91/24
                    src-ip 10.10.10.106/24
                exit
                action drop
            exit
            entry 2 create
...
----------------------------------------------
A:ALA-7>config>filter#
```

Filter Command Reference

Command Hierarchies

Configuration Commands

IP Filter Policy Commands

config
— **filter**
— **ip-filter** *filter-id* [**use-ipv6-resource**] [**create**]
— **no ip-filter** *filter-id*
— **default-action** {**drop** | **forward**}
— **description** *description-string*
— **no description**
— **renum** *old-entry-id new-entry-id*
— **scope** {**exclusive** | **template**}
— **no scope**
— **entry** *entry-id* [**time-range** *time-range-name*] [**create**]
— **no entry** *entry-id*
— **action**[**drop**]
— **action forward**
— **no action**
— **description** *description-string*
— **no description**
— **match** [**protocol** *protocol-id*]
— **no match**
— **dscp** *dscp-name*
— **no dscp**
— **dst-ip** {*ip-address/mask* | *ip-address netmask*}
— **no dst-ip**
— **dst-port** {**eq**} *dst-port-number*
— **dst-port range**
— **no dst-port**
— **fragment** {**true** | **false**}
— **no fragment**
— **icmp-code** *icmp-code*
— **no icmp-code**
— **icmp-type** *icmp-type*

— **no icmp-type**
— **option-present** {**true** | **false**}
— **no option-present**
— **src-ip**{*ip-address/mask* | *ip-address netmask*}
— **no src-ip**
— **src-port** {{**eq**} *src-port-number*
— **no src-port**
— **tcp-ack** {**true** | **false**}
— **no tcp-ack**
— **tcp-syn** {**true** | **false**}
— **no tcp-syn**

IPv6 Filter Policy Commands

config
- — **filter**
  - — **ipv6-filter** *ipv6-filter-id* **[ipv6-128bit-address | ipv6-64bit-address] [create]**
  - — **no ipv6-filter** *ipv6-filter-id*
    - — **default-action** {**drop** | **forward**}
    - — **description** *description-string*
    - — **no description**
    - — **entry** *entry-id* [**time-range** *time-range-nam*e] **[create]**
    - — **no entry** *entry-id*
      - — **action** {**drop** | **forward**}
      - — **no action**
      - — **description** *description-string*
      - — **no description**
      - — **match** [**next-header** *next-header*]
      - — **no match**
        - — **dscp** *dscp-name*
        - — **no dscp**
        - — **dst-ip** [*ipv6-address/prefix-length*]
        - — **dst-ip no**
        - — **dst-port** {**eq**} *dst-port-number*
        - — **no dst-port**
        - — **icmp-code** *icmp-code*
        - — **no icmp-code**
        - — **icmp-type** *icmp-type*
        - — **no icmp-type**
        - — **dst-ip** {*ipv6-address/prefix-length*}
        - — **dst-ipno**
        - — **src-port** { **eq**} *src-port-number*
        - —
        - — **src-port range** *start end*}
        - — **no src-port**
        - — **no src-ip**
        - — **src-ip [ipv6-address/prefix-length]**
        - — **tcp-ack** {**true** | **false**}
        - — **no tcp-ack**
        - — **tcp-syn** {**true** | **false**}
        - — **no tcp-syn**
    - — **renum** *old-entry-id new-entry-id*
    - — **scope** {**exclusive** | **template**}
    - — **no scope**

MAC Filter Policy Commands

config
- **filter**
  - **mac-filter** *filter-id* [**create**]
  - **no mac-filter** *filter-id*
    - **default-action** {**drop** | **forward**}
    - **description** *description-string*
    - **no description**
    - **entry** *entry-id* [**time-range** *time-range-name*]
    - **no entry** *entry-id*
      - **description** *description-string*
      - **no description**
      - **action** [**drop**]
      - **action forward**
      - **no action**
      - **match**
      - **no match**
        - **dot1p** *dot1p-value* [*dot1p-mask*]
        - **no dot1p**
        - **dst-mac** *ieee-address* [*ieee-address-mask*]
        - **no dst-mac**
        - **etype** *0x0600..0xffff*
        - **no etype**
        - **src-mac** *ieee-address* [*ieee-address-mask*]
        - **no src-mac**
    - **renum** *old-entry-id new-entry-id*
    - **scope** {**exclusive** | **template**}
    - **no scope**

Generic Filter Commands

config
— **filter**
— **copy** *ip-filter* | *mac-filter src-filter-id* [**src-entry** *src-entry-id*] **to** *dst-filter-id* [**dst-entry** *dst-entry-id*] [**overwrite**]

Show Commands

show
— **filter**
— **download-failed**
— **ip** [*ip-filter-id* [**entry** *entry-id*] [**association** | **counters**]
— **ipv6** [*ipv6-filter-id* [**entry** *entry-id*] [**association** | **counters**]]
— **mac** {*mac-filter-id* [**entry** *entry-id*] [**association** | **counters**]}

Clear Commands

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

Monitor Commands

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

Configuration Commands

Generic Commands

description

Syntax **description** *string*
no description

Context config>filter>ip-filter
config>filter>ip-filter>entry
config>filter>ipv6-filter
config>filter>ipv6-filter>entry
config>filter>mac-filter
config>filter>mac-filter>entry

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

The **description** command associates a text string with a configuration context to help identify the context in the configuration file.

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

Default none

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

Global Filter Commands

ip-filter

Syntax [**no**] **ip-filter** *filter-id* **[use-ipv6-resource] [create]**

Context config>filter

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

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

The IP filter policy, sometimes referred to as an access control list (ACL), is a template that can be applied to multiple services or multiple network ports as long as the scope of the policy is template.

Any changes made to the existing policy, using any of the sub-commands, will be applied immediately to all services where this policy is applied. For this reason, when many changes are required on an ip-filter policy, it is recommended that the policy be copied to a work area. That work-in-progress policy can be modified until complete and then written over the original filter policy. Use the **config filter copy** command to maintain policies in this manner.

Use-ipv6-resource - By default, when an IPv4 filter policy is associated with a service entity (For example: SAP), the software attempts to allocate resources for the filter policy entries from the IPv4 resource pool. If resources unavailable in the pool, then the software fails to associate and display an error. If the user knows that resources are free in the IPv6 resource pool, then the use-ipv6-resource parameter is used to allow the user to share the entries in the resource chunks allocated for use by IPv6 128-bit resource pool, if available. If this parameter is specified then the resource for this filter policy is always allocated from the IPv6 128-bit filter resource pool.

Note: By default, IPv4 filters are created using IPv4 resources, assuming an unspecified use-ipv6-resource. If such filters are to be created using IPv6 resources, the use-ipv6-resource option needs to be specified. Ahead of the application of such a filter, the user should ensure the number of policies in the newly created policy is within the limit of available resources in the IPv6 128-bit resource pool, by considering the dump of "tools>dump# system-resources" command.

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

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

Values 1 — 65535

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

use-ipv6-resource — Indicates to the system that the hardware resources for the entries in this filter policy must be allocated from the IPv6 filter resource pool, if available. For more information see the CLI description above.

ipv6-filter

Syntax **[no] ipv6-filter** *ipv6-filter-id* **[ipv6-128bit-address | ipv6-64bit-address] [create]**

Context config>filter

Description This command enables the context to create IPv6 filter policy. During the 'create', the user must specify if IPv6 addresses, both source and destination IPv6 addresses, specified in the match criteria uses complete 128-bits or uses only the upper 64 bits of the IPv6 addresses.

The **no** form of the command deletes the IPv6 filter policy. A filter policy cannot be deleted until it is removed from all SAPs or network ports where it is applied

Default By default IPv6 filter policy allows the use of 128-bit addresses.

Parameters *ipv6-filter-id* — The IPv6 filter policy ID number.

Values 1 — 65535

ipv6-128bit-address — If the user intends to use complete 128-bit addresses, then the user requires the ipv6-128bit-address CLI parameter with the create command. When this policy is associated with a SAP, software allocates resources for the filter entries from the IPv6 128-bit resource pool for the SAP.

ipv6-64bit-address — If the user intends to use upper most significant bit(MSB) 64-bit addresses, hen the user requires the ipv6-64bit-address CLI parameter with the create command. When this policy is associated with a SAP, software allocates resources for the filter entries from the IPv6 64-bit resource pool for the SAP. All the IP packet fields are not available for match are when using 64-bit addresses. For more information, see Configuration Notes on page 228, to know the packet header fields available formatch when using this option.

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

mac-filter

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

Context config>filter

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

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

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

Note it is not possible to apply a MAC filter policy to a network port network IP interface.

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. For this reason, when many changes are required on a mac-filter policy, it is recommended that the policy be copied to a work area. That work-in-progress policy can be modified until complete and then written over the original filter policy. Use the **config filter copy** command to maintain policies in this manner.

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

Parameters *filter-id* — The MAC filter policy ID number.

Values 1 — 65535

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

Filter Policy Commands

default-action

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

Context config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-filter

Description This command specifies the action to be applied to packets when the packets do not match the specified criteria in all of the IP filter entries of the filter.

When multiple **default-action** commands are entered, the last command will overwrite the previous command.

Default drop

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

forward — Specifies all packets will be forwarded unless there is a specific filter entry which causes the packet to be dropped.

scope

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

Context 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 services or 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 (SAP or network IP interface). Attempting to assign the policy to a second entity will result in an error message. 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 SAPs or network IP interfaces.

General Filter Entry Commands

entry

Syntax **entry** *entry-id* [**time-range** *time-range-name*] [**create**]
no entry *entry-id*

Context config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-filter

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

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

The **no** form of the command removes the specified entry from the IP or MAC filter. Entries removed from the IP or MAC filter are ediately removed from all services or network ports where that filter is applied.

Default none

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

Values 1 — 65535

time-range *time-range-name* **—** Specifies the time range name to be associated with this filter entry up to 32 characters in length. The time-range name must already exist in the config>cron context.

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

IP Filter Entry Commands

action

Syntax **action** [**drop**]
action forward
no action

Context config>filter>ip-filter>entry
config>filter>ipv6-filter>entry

Description This command specifies to match packets with a specific IP option or a range of IP options in the first option of the IP header as an IP filter match criterion. The **action** keyword must be entered and a keyword specified in order for the entry to be active.

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

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

Default none

Parameters **drop** — Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded.

match

Syntax **match** [**protocol** *protocol-id*]
no match

Context config>filter>ip-filter>entry
config>filter>ipv6-filter>entry

Description This command enables the context to enter match criteria for the filter entry. When the match criteria have been satisfied the action associated with the match criteria is executed.

If more than one match criteria (within one match statement) are configured then all criteria must be satisfied (AND function) before the action associated with the match is executed.

A **match** context may consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

The **no** form of the command removes the match criteria for the *entry-id*.

Parameters **protocol** — The **protocol** keyword configures an IP protocol to be used as an IP filter match criterion. The protocol type such as TCP or UDP is identified by its respective protocol number.

protocol-id — Configures the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP(1), TCP(6), UDP(17). The **no** form the command removes the protocol from the match criteria.

Values 0 — 255 (values can be expressed in decimal, hexidecimal, or binary - DHB)
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
* — udp/tcp wildcard

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	Any private interior gateway (used by Cisco for IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Spanning Tree Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram

MAC Filter Entry Commands

action

Syntax **action drop**
action forward
no action

Context config>filter>mac-filter>entry

Description This command configures the action for a MAC filter entry. The **action** keyword must be entered for the entry to be active. Any filter entry without the **action** keyword will be considered incomplete and will be inactive.

If neither drop nor forward is specified, this is considered a No-Op filter entry used to explicitly set a filter entry inactive without modifying match criteria or removing the entry itself.

Multiple action statements entered will overwrite previous actions parameters when defined. To remove a parameter, use the no form of the action command with the specified parameter.

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

Default none

Parameters **drop** — Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded.

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

match

Syntax **match**
no match

Context config>filter>mac-filter>entry

Description This command creates the context for entering/editing match criteria for the filter entry and specifies an Ethernet frame type for the entry. When the match criteria have been satisfied the action associated with the match criteria is executed.

If more than one match criteria (within one match statement) are configured then all criteria must be satisfied (AND function) before the action associated with the match 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*.

Parameters **frame-type** *keyword* **—** The **frame-type** keyword configures an Ethernet frame type to be used for the MAC filter match criteria.

Default **ethernet_II**

IP Filter Match Criteria

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* — Configure 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*]} [*netmask*]
no dst-ip
dst-ip {*ip-address*/prefix-length]
no dst-ip

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

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

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

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

Default none

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

Values 0.0.0.0 — 255.255.255.255

ipv6-address — The IPv6 prefix for the IP match criterion in dotted decimal notation.

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..FFFF]H
d: [0..255]D

mask — The subnet mask length expressed as a decimal integer.

Values 0 — 32

netmask — Any mask epressed in dotted quad notation.

Values 0.0.0.0 — 255.255.255.255

Values

dst-port

Syntax **dst-port** {**eq**} *dst-port-number*
no dst-port

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures a destination TCP or UDP port number for an IP filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

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

Default **none**

Parameters **eq —** Specifies the operator to use relative to *dst-port-number* for specifying the port number match criteria. The **eq** keyword 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 — 65535

fragment

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

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

Description Configures fragmented or non-fragmented IP packets as an IP filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

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

Default **no fragment**

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

false — Configures a match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.

icmp-code

Syntax **icmp-code** *icmp-code*
no icmp-code

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description Configures matching on ICMP code field in the ICMP header of an IP packet as a filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

This option is only meaningful if the protocol match criteria specifies ICMP (1).

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

Default **no icmp-code**

Parameters *icmp-code* — The ICMP code values that must be present to match.

Values 0 — 255

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context 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 IP or packet as a filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

This option is only meaningful if the protocol match criteria specifies ICMP (1).

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

Default **no icmp-type**

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

Values 0 — 255

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 zero in the IP header as an IP filter match criterion.

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

Parameters **true —** Specifies matching on all IP packets that contain the option field in the header. A match will occur for all packets that have the option field present. An option field of zero is considered as no option present.

false — Specifies matching on IP packets that do not have any option field present in the IP header. (an option field of zero). An option field of zero is considered as no option present.

src-ip

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

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

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

To match on the source IP address, specify the address and its associated mask, e.g. 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

If the filter is created to match 64-bit address, then the IPv6 address specified for the match must contain only first 64-bits (i.e. first 4 16-bit groups of the IPv6 address).

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

Default **no src-ip**

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

Values 0.0.0.0 — 255.255.255.255

mask — The subnet mask length expressed as a decimal integer.

Values 0 — 32

netmask — Any mask epressed in dotted quad notation.

Values 0.0.0.0 — 255.255.255.255

Values

src-port

Syntax **src-port** {**eq**} *src-port-number*
no src-port

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures a source TCP or UDP port number for an IP filter match criterion. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

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

Default no src-port

Parameters **eq —** Specifies the operator to use relative to *src-port-number* for specifying the port number match criteria. The **eq** keyword 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 0 — 65535

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. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

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. Note that an entry containing L4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the L4 information.

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.

MAC Filter Match Criteria

dot1p

Syntax **dot1p** *ip-value* [*mask*]
no dot1p

Context config>filter>mac-filter>entry>match

Description Configures an IEEE 802.1p value or range to be used as a MAC filter match criterion.

When a frame is missing the 802.1p bits, specifying an dot1p match criterion will fail for the frame and result in a non-match for the MAC filter entry.

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

The MAC filter applied on the SAP egress can match the details of the packet-on-the-wire. For example, a QinQ packet came in on a null SAP and egressing on a Dot1p-encapsulated port, the packet-on-the-wire will have three tags. Now, the etype=0x8100 and Dot1p will equal the outer VLAN tag's Dot1p. This Etype and Dot1p can be configured on the egress filter to match this packet.

Default no dot1p

Parameters *ip-value* — The IEEE 802.1p value in decimal.

Values 0 — 7

mask — This 3-bit mask can be configured using the following formats:

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

To select a range from 4 up to 7 specify *p-value* of 4 and a *mask* of 0b100 for value and mask.

Default **7 (decimal)**

Values 1 — 7 (decimal)

Values

dst-mac

Syntax **dst-mac** *ieee-address* [*mask*]
no dst-mac

Context config>filter>mac-filter>entry>match

Description Configures a destination MAC address or range to be used as a MAC filter match criterion.

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

Default no dst-mac

Parameters *ieee-address* — The MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

mask — A 48-bit mask to match a range of MAC address values.

This 48-bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0xFFFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 0003FA000000 0x0FFFFF000000

Default **0xFFFFFFFFFFFF (exact match)**

Values 0x00000000000000 — 0xFFFFFFFFFFFF

etype

Syntax **etype** *ethernet-type*
no etype

Context config>filter>mac-filter>entry>match

Description Configures an Ethernet type II Ethertype value to be used as a MAC filter match criterion.

The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. For example, 0800 is used to identify the IPv4 packets.

The Ethernet type field is used by the Ethernet version-II frames. IEEE 802.3 Ethernet frames do not use the type field. Table 9, MAC Match Criteria Exclusivity Rules, on page 111 describes fields that are exclusive based on the frame format.

The **no** form of the command removes the previously entered etype field as the match criteria.

Default no etype

Parameters *ethernet-type* — The Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.

Values 0x0600 — 0xFFFF

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context config>filter>mac-filter>entry

Description Configures a source MAC address or range to be used as a MAC filter match criterion.

The **no** form of the command removes the source mac as the match criteria.

Default no src-mac

Parameters *ieee-address* — Enter the 48-bit IEEE mac address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — This 48-bit mask can be configured using:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0x0FFFFF000000
Binary	0bBBBBBBB...B	0b11110000...B

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 003FA000000 0xFFFFFF000000

Default **0xFFFFFFFFFFFF** (exact match)

Values 0x00000000000000 — 0xFFFFFFFFFFFF

Policy and Entry Maintenance Commands

copy

Syntax **copy** {**ip-filter | mac-filter**} *source-filter-id dest-filter-id dest-filter-id* [**overwrite**]

Context config>filter

Description This command copies existing filter list entries for a specific filter ID to another filter ID. The **copy** command is a configuration level maintenance tool used to create new filters using existing filters. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.
If **overwrite** is not specified, an error will occur if the destination policy ID exists.

Parameters **ip-filter —** Indicates that the *source-filter-id* and the *dest-filter-id* are IP filter IDs.

mac-filter — Indicates that the *source-filter-id* and the *dest-filter-id* are MAC filter IDs.

source-filter-id — The *source-filter-id* identifies the source filter policy from which the copy command will attempt to copy. The filter policy must exist within the context of the preceding keyword (**ip-filter** or **mac-filter**).

dest-filter-id — The *dest-filter-id* identifies the destination filter policy to which the copy command will attempt to copy. If the **overwrite** keyword does not follow, the filter policy ID cannot already exist within the system for the filter type the copy command is issued for. If the **overwrite** keyword is present, the destination policy ID may or may not exist.

overwrite — The **overwrite** keyword specifies that the destination filter ID may exist. If it does, everything in the existing destination filter ID will be completely overwritten with the contents of the source filter ID. If the destination filter ID exists, either **overwrite** must be specified or an error message will be returned. If **overwrite** is specified, the function of copying from source to destination occurs in a 'break before make' manner and therefore should be handled with care.

renum

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

Context config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-filter

Description This command renumbers existing MAC or IP filter entries to properly sequence filter entries.
This may be required in some cases since the OS exits when the first match is found and executes the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

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

Values 1 — 65535

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

Values 1 — 65535

Show Commands

download-failed

Syntax **download-failed**

Context show>filter

Description This command shows all filter entries for which the download has failed.

Output **download-failed Output —** The following table describes the filter download-failed output.

Label	Description
`Filter-type`	Displays the filter type.
`Filter-ID`	Displays the ID of the filter.
`Filter-Entry`	Displays the entry number of the filter.

Sample Output

```
A:ALA-48# show filter download-failed
============================================
Filter entries for which download failed
============================================
Filter-type    Filter-Id      Filter-Entry
--------------------------------------------
ip              1          10
============================================
A:ALA-48#
```

ip

Syntax ip <ip-filter-id> [association|counters]
ip <ip-filter-id> entry <entry-id> [counters]

Context show>filter

Description This command shows IP filter information.

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

Values 1 — 65535

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

Values 1 — 65535

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

counters — Displays counter information for the specified filter ID. Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.

type *entry-type* — Displays information on the specified filter ID for the specified *entry-type* only

Output **Show Filter (no filter-id specified) —** The following table describes the command output for the command when no filter ID is specified.

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

Sample Output

```
A:ALA-49# show filter ip
===============================================================================
IP Filters
===============================================================================
Filter-Id Scope    Applied Description
-------------------------------------------------------------------------------
1         Template Yes
3         Template Yes
6         Template Yes
10        Template No
11        Template No
-------------------------------------------------------------------------------
Num IP filters: 5
===============================================================================
A:ALA-49#

*A:Dut-C>config>filter# show filter ip
===============================================================================
IP Filters                                                       Total:     2
===============================================================================
Filter-Id   Scope    Applied Description
-------------------------------------------------------------------------------
10001       Template Yes
fSpec-1     Template Yes     BGP FlowSpec filter for the Base router
-------------------------------------------------------------------------------
Num IP filters: 2
===============================================================================
```

```
*A:Dut-C>config>filter#
```

Output **Show Filter (with filter-id specified) —** The following table describes the command output for the command when a filter ID is specified.

Label	Description
`Filter Id`	The IP filter policy ID.
`Scope`	`Template` – The filter policy is of type template.
	`Exclusive` – The filter policy is of type exclusive.
`Entries`	The number of entries configured in this filter ID.
`Description`	The IP filter policy description.
`Applied`	`No` – The filter policy ID has not been applied.
	`Yes` – The filter policy ID is applied.
`Def. Action`	`Forward` – The default action for the filter ID for packets that do not match the filter entries is to forward.
	`Drop` – The default action for the filter ID for packets that do not match the filter entries is to drop.
`Filter Match Criteria`	`IP` – Indicates the filter is an IP filter policy.
`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.
`ICMP Type`	The ICMP type match criterion. `Undefined` indicates no ICMP type specified.
`Fragment`	`False` – Configures a match on all non-fragmented IP packets.
	`True` – Configures a match on all fragmented IP packets.
	`Off` – Fragments are not a matching criteria. All fragments and non-fragments implicitly match.
`TCP-syn`	`False` – Configures a match on packets with the SYN flag set to false.
	`True` – Configured a match on packets with the SYN flag set to true.
	`Off` – The state of the TCP SYN flag is not considered as part of the match criteria.
`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.

Label	Description (Continued)
	Forward — The explicit action to perform is forwarding of the packet.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Src. Port	The source TCP or UDP port number.
Dest. Port	The destination TCP or UDP port numbere.
Dscp	The DiffServ Code Point (DSCP) name.
ICMP Code	The ICMP code field in the ICMP header of an IP packet.
Option-present	Off — Specifies not to 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 be used as IP filter match criteria.
TCP-ack	False — Configures a match on packets with the ACK flag set to false.
	True — Configurs a match on packets with the ACK flag set to true.
	Off — The state of the TCP ACK flag is not considered as part of the match criteria. as part of the match criteria.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

Sample Output

```
A:ALA-49>config>filter# show filter ip 3
===============================================================================
IP Filter
===============================================================================
Filter Id    : 3                                Applied        : Yes
Scope        : Template                         Def. Action    : Drop
Entries      : 1
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry        : 10
Src. IP      : 10.1.1.1/24                      Src. Port      : None
Dest. IP     : 0.0.0.0/0                        Dest. Port     : None
Protocol     : 2                                Dscp           : Undefined
ICMP Type    : Undefined                        ICMP Code      : Undefined
TCP-syn      : Off                              TCP-ack        : Off
Match action : Drop
Ing. Matches : 0                                Egr. Matches   : 0
===============================================================================
A:ALA-49>config>filter#

*A:Dut-C>config>filter# show filter ip fSpec-1 associations
===============================================================================
```

```
IP Filter
===============================================================================
Filter Id    : fSpec-1                          Applied        : Yes
Scope        : Template                         Def. Action    : Forward
Radius Ins Pt: n/a
CrCtl. Ins Pt: n/a
Entries      : 2 (insert By Bgp)
Description  : BGP FlowSpec filter for the Base router
-------------------------------------------------------------------------------
Filter Association : IP
-------------------------------------------------------------------------------
Service Id   : 1                                Type           : IES
- SAP    1/1/3:1.1   (merged in ip-fltr 10001)
===============================================================================
*A:Dut-C>config>filter#


*A:Dut-C>config>filter# show filter ip 10001
===============================================================================
IP Filter
===============================================================================
Filter Id    : 10001                            Applied        : Yes
Scope        : Template                         Def. Action    : Drop
Radius Ins Pt: n/a
CrCtl. Ins Pt: n/a
Entries      : 1
BGP Entries  : 2
Description  : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry        : 1
Description  : (Not Specified)
Log Id       : n/a
Src. IP      : 0.0.0.0/0                        Src. Port      : None
Dest. IP     : 0.0.0.0/0                        Dest. Port     : None
Protocol     : 6                                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 : Forward
Next Hop     : Not Specified
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

Entry        : fSpec-1-32767  - inserted by BGP FLowSpec
Description  : (Not Specified)
Log Id       : n/a
Src. IP      : 0.0.0.0/0                        Src. Port      : None
Dest. IP     : 0.0.0.0/0                        Dest. Port     : None
Protocol     : 6                                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 pkts
Egr. Matches : 0 pkts

Entry        : fSpec-1-49151  - inserted by BGP FLowSpec
Description  : (Not Specified)
Log Id       : n/a
Src. IP      : 0.0.0.0/0                       Src. Port      : None
Dest. IP     : 0.0.0.0/0                       Dest. Port     : None
Protocol     : 17                              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 pkts
Egr. Matches : 0 pkts

===============================================================================
*A:Dut-C>config>filter#
```

Output **Show Filter (with time-range specified) —** If a time-range is specified for a filter entry, the following is displayed.

```
A:ALA-49# show filter ip  10
===============================================================================
IP Filter
===============================================================================
Filter Id    : 10                              Applied        : No
Scope        : Template                        Def. Action    : Drop
Entries      : 2
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry        : 1010
time-range   : day                             Cur. Status    : Inactive
Src. IP      : 0.0.0.0/0                       Src. Port      : None
Dest. IP     : 10.10.100.1/24                  Dest. Port     : None
Protocol     : Undefined                       Dscp           : Undefined
ICMP Type    : Undefined                       ICMP Code      : Undefined
Fragment     : Off                             Option-present : Off
TCP-syn      : Off                             TCP-ack        : Off
Match action : Forward
Ing. Matches : 0                               Egr. Matches   : 0

Entry        : 1020
time-range   : night                           Cur. Status    : Active
Src. IP      : 0.0.0.0/0                       Src. Port      : None
Dest. IP     : 10.10.1.1/16                    Dest. Port     : None
Protocol     : Undefined                       Dscp           : Undefined
ICMP Type    : Undefined                       ICMP Code      : Undefined
Fragment     : Off                             Option-present : Off
TCP-syn      : Off                             TCP-ack        : Off
Match action : Forward
Ing. Matches : 0                               Egr. Matches   : 0
===============================================================================
A:ALA-49#
```

Output **Show Filter Associations —** The following table describes the fields that display when the **associations** keyword is specified.

Label	Description
Filter Id	The IP filter policy ID.
Scope	Template — The filter policy is of type Template.
	Exclusive — The filter policy is of type Exclusive.
Entries	The number of entries configured in this filter ID.
Applied	No — The filter policy ID has not been applied.
	Yes — The filter policy ID is applied.
Def. Action	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.
Service Id	The service ID on which the filter policy ID is applied.
SAP	The Service Access Point on which the filter policy ID is applied.
(Ingress)	The filter policy ID is applied as an ingress filter policy on the interface.
(Egress)	The filter policy ID is applied as an egress filter policy on the interface.
Type	The type of service of the service ID.

Sample Output

```
A:ALA-49# show filter ip 1 associations
===============================================================================
IP Filter
===============================================================================
Filter Id    : 1                                Applied        : Yes
Scope        : Template                         Def. Action    : Drop
Entries      : 1
-------------------------------------------------------------------------------
Filter Association : IP
-------------------------------------------------------------------------------
Service Id   : 1001                             Type           : VPLS
 - SAP    1/1/1:1001   (Ingress)
Service Id   : 2000                             Type           : Epipe
 - SAP    1/1/1:2000   (Ingress)
===============================================================================
A:ALA-49#
```

Output **Show Filter Associations (with TOD-suite specified) —** If a filter is referred to in a TOD Suite assignment, it is displayed in the show filter associations command output:

```
A:ALA-49# show filter ip 160 associations
===============================================================================
IP Filter
===============================================================================
Filter Id    : 160                          Applied        : No
Scope        : Template                     Def. Action    : Drop
Entries      : 0
-------------------------------------------------------------------------------
Filter Association : IP
-------------------------------------------------------------------------------
Tod-suite "english_suite"
 - ingress, time-range "day" (priority 5)
===============================================================================
A:ALA-49#
```

Output **Show Filter Counters —** The following table describes the output fields when the **counters** keyword is specified..

Label	Description
IP Filter Filter Id	The IP filter policy 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.
Def. Action	Forward — The default action for the filter ID for packets that do not match the filter entries is to forward.
	Drop — The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	IP — Indicates the filter is an IP filter policy.
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.
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.
	Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.

ipv6

Syntax **ipv6 {***ipv6-filter-id* **[entry** *entry-id***] [association | counters]}**

Context show>filter

Description This command shows IPv6 filter information.

Parameters *ipv6-filter-id* — Displays detailed information for the specified IPv6 filter ID and filter entries.

Values 1 — 65535

entry entry-id — Displays information on the specified IPv6 filter entry ID for the specified filter ID.

Values 1 — 9999

associations — Appends information as to where the IPv6 filter policy ID is applied to the detailed filter policy ID output.

counters — Displays counter information for the specified IPv6 filter ID.

Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.

Output **Show Filter (no filter-id specified) —** The following table describes the command output for the command when no filter ID is specified.

Table 13: Show Filter (no filter-id specified)

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

Sample Output

```
*A:7210SAS>show>filter# ipv6

===============================================================================
IPv6 Filters                                                     Total:     1
===============================================================================
Filter-Id Scope    Applied Description
-------------------------------------------------------------------------------
1         Template Yes
-------------------------------------------------------------------------------
Num IPv6 filters: 1
===============================================================================
*A:7210SAS>show>filter#
```

Output **Show Filter (with filter-id specified) —** The following table describes the command output for the command when a filter ID is specified.

Table 14: Show Filter (with filter-id specified)

Label	Description
`Filter Id`	The IP filter policy ID.
`Scope`	`Template` — The filter policy is of type template. `Exclusive` — The filter policy is of type exclusive.
`Entries`	The number of entries configured in this filter ID.
`Description`	The IP filter policy description.
`Applied`	No — The filter policy ID has not been applied. Yes — The filter policy ID is applied.
`Def. Action`	Forward — The default action for the filter ID for packets that do not match the filter entries is to forward. Drop — The default action for the filter ID for packets that do not match the filter entries is to drop.
`Filter Match Criteria`	IP — Indicates the filter is an IP filter policy.
`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.
`Src. IP`	The source IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
`Dest. IP`	The destination IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
`ICMP Type`	The ICMP type match criterion. Undefined indicates no ICMP type specified.
IP-Option	Specifies matching packets with a specific IP option or a range of IP options in the IP header for IP filter match criteria.
`TCP-syn`	False — Configures a match on packets with the SYN flag set to false. True — Configured a match on packets with the SYN flag set to true. Off — The state of the TCP SYN flag is not considered as part of the match criteria.

Table 14: Show Filter (with filter-id specified)

Match action	Default — The filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified. Drop — Drop packets matching the filter entry. Forward — The explicit action to perform is forwarding of the packet. If the action is Forward, then if configured the nexthop information should be displayed, including Nexthop: <IP address>, Indirect: <IP address> or Interface: <IP interface name>.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Src. Port	The source TCP or UDP port number or port range.
Dest. Port	The destination TCP or UDP port number or port range.
Dscp	The DiffServ Code Point (DSCP) name.
ICMP Code	The ICMP code field in the ICMP header of an IP packet.
TCP-ack	False — Configures a match on packets with the ACK flag set to false. True — Configured a match on packets with the ACK flag set to true. Off — The state of the TCP ACK flag is not considered as part of the match criteria
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Egr. Matches	The number of egress filter matches or hits for the filter entry.

Sample Output

```
*A:7210SAS>show>filter# ipv6 1

===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 1                                Applied        : Yes
Scope        : Template                         Def. Action    : Drop
Entries      : 2
Description  : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry        : 1
Description  : Test
Src. IP      : 1::1/128                         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 : Forward
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

Entry        : 2
Description  : (Not Specified)
Src. IP      : ::/0                             Src. Port     : None
Dest. IP     : 1:2::1AFC/128                    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 : 819 pkts
Egr. Matches : 0 pkts

===============================================================================
*A:7210SAS>show>filter#
```

Output **Show Filter Associations** — The following table describes the fields that display when the associations keyword is specified.

Table 15: Show Filter Associations

Label	Description
`Filter Id`	The IPv6 filter policy ID.
`Scope`	Template — The filter policy is of type Template. Exclusive — The filter policy is of type Exclusive.
`Entries`	The number of entries configured in this filter ID.
`Applied`	No — The filter policy ID has not been applied. Yes — The filter policy ID is applied.
`Def. Action`	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.
`Description`	The IP filter policy description.
`Service Id`	The service ID on which the filter policy ID is applied.
`SAP`	The Service Access Point on which the filter policy ID is applied. (Ingress) The filter policy ID is applied as an ingress filter policy on the interface. (Egress) The filter policy ID is applied as an egress filter policy on the interface.
`Type`	The type of service of the service ID.

Sample Output

```
*A:7210SAS>show>filter# ipv6 1 associations

===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 1                                Applied        : Yes
Scope        : Template                         Def. Action    : Drop
Entries      : 2
Description  : (Not Specified)
-------------------------------------------------------------------------------
Filter Association : IPv6
-------------------------------------------------------------------------------
Service Id   : 1                                Type           : Epipe
 - SAP    1/1/1:1   (Ingress)
Service Id   : 2                                Type           : VPLS
 - SAP    1/1/1:2   (Ingress)
 - SAP    1/1/1:3   (Ingress)
===============================================================================
*A:7210SAS>show>filter#
```

Output **Show Filter Counters** — The following table describes the output fields when the counterskeyword is specified.

Table 16: Show Filter Counters

Label	Description
`Filter Id`	The IPv6 filter policy ID.
`Scope`	Template — The filter policy is of type Template. Exclusive — The filter policy is of type Exclusive.
`Entries`	The number of entries configured in this filter ID.
`Applied`	No — The filter policy ID has not been applied. Yes — The filter policy ID is applied.
`Def. Action`	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.
`Description`	The IP filter policy description.
`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.

Table 16: Show Filter Counters

`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. Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.

Sample Output

```
*A:7210SAS>show>filter# ipv6 1 counters

===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 1                               Applied        : Yes
Scope        : Template                        Def. Action    : Drop
Entries      : 2
Description  : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry        : 1
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

Entry        : 2
Ing. Matches : 819 pkts
Egr. Matches : 0 pkts

===============================================================================
*A:7210SAS>show>filter#
```

mac

Syntax **mac** [*mac-filter-id* [**associations | counters**] [**entry** *entry-id*]]

Context show>filter

Description This command displays MAC filter information.

Parameters *mac-filter-id* — Displays detailed information for the specified filter ID and its filter entries.

Values 1— 65535

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

counters — Displays counter information for the specified filter ID.

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

Values 1 — 65535

Output **No Parameters Specified —** When no parameters are specified, a brief listing of IP filters is produced. The following table describes the command output for the command.

Filter ID Specified — When the filter ID is specified, detailed filter information for the filter and its entries is produced. The following table describes the command output for the command.

Label	Description
`MAC Filter Filter Id`	The MAC filter policy ID.
`Scope`	`Template` – The filter policy is of type Template. `Exclusive` – The filter policy is of type Exclusive.
`Description`	The IP filter policy description.
`Applied`	`No` – The filter policy ID has not been applied. `Yes` – The filter policy ID is applied.
`Def. Action`	`Forward` – The default action for the filter ID for packets that do not match the filter entries is to forward. `Drop` – The default action for the filter ID for packets that do not match the filter entries is to drop.
`Filter Match Criteria`	`MAC` – Indicates the filter is an MAC filter policy.
`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.
`Description`	The filter entry description.
`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.
`Src MAC`	The source MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion specified for the filter entry.
`Dest MAC`	The destination MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion specified for the filter entry.
`Dot1p`	The IEEE 802.1p value for the match criteria. `Undefined` indicates no value is specified.
`Ethertype`	The Ethertype value match criterion.

Label	Description (Continued)
`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 is forwarded.
`Ing. Matches`	The number of ingress filter matches/hits for the filter entry.
`Egr. Matches`	The number of egress filter matches/hits for the filter entry.

Sample Detailed Output

```
===============================================================================
Mac Filter : 200
===============================================================================
Filter Id     : 200                              Applied       : No
Scope         : Exclusive                        D. Action     : Drop
Description : Forward SERVER sourced packets
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
-------------------------------------------------------------------------------
Entry          : 200                             FrameType     : 802.2SNAP
Description    : Not Available
Src Mac        : 00:00:5a:00:00:00 ff:ff:ff:00:00:00
Dest Mac       : 00:00:00:00:00:00 00:00:00:00:00:00
Dot1p          : Undefined                       Ethertype     : 802.2SNAP
Match action   : Forward
Ing. Matches   : 0                               Egr. Matches  : 0
Entry          : 300 (Inactive)                  FrameType     : Ethernet
Description    : Not Available
Src Mac        : 00:00:00:00:00:00 00:00:00:00:00:00
Dest Mac       : 00:00:00:00:00:00 00:00:00:00:00:00
Dot1p          : Undefined                       Ethertype     : Ethernet
Match action   : Default
Ing. Matches   : 0                               Egr. Matches  : 0
===============================================================================
```

Filter Associations — The associations for a filter ID will be displayed if the **associations** keyword is specified. The assocation information is appended to the filter information. The following table describes the fields in the appended associations output.

Label	Description
`Filter Association`	`Mac` — The filter associations displayed are for a MAC filter policy ID.
`Service Id`	The service ID on which the filter policy ID is applied.
`SAP`	The Service Access Point on which the filter policy ID is applied.
`Type`	The type of service of the Service ID.

Label	Description (Continued)
`(Ingress)`	The filter policy ID is applied as an ingress filter policy on the interface.
`(Egress)`	The filter policy ID is applied as an egress filter policy on the interface.

Sample Output

```
A:ALA-49# show filter mac 3 associations
===============================================================================
Mac Filter
===============================================================================
Filter ID : 3                                Applied       : Yes
Scope     : Template                         Def. Action   : Drop
Entries   : 1
-------------------------------------------------------------------------------
Filter Association : Mac
-------------------------------------------------------------------------------
Service Id: 1001                             Type          : VPLS
- SAP 1/1/1:1001   (Egress)
===============================================================================
A:ALA-49#
```

Filter Entry Counters Output — When the **counters** keyword is specified, the filter entry output displays the filter matches/hit information. The following table describes the command output for the command.

```
A:ALA-49# show filter mac 8 counters
```

Label	Description
`Mac Filter Filter Id`	The MAC filter policy ID.
`Scope`	`Template` – The filter policy is of type Template.
	`Exclusive` – The filter policy is of type Exclusive.
`Description`	The MAC filter policy description.
`Applied`	`No` – The filter policy ID has not been applied.
	`Yes` – The filter policy ID is applied.
`Def. Action`	`Forward` – The default action for the filter ID for packets that do not match the filter entries is to forward.
	`Drop` – The default action for the filter ID for packets that do not match the filter entries is to drop.
`Filter Match Criteria`	`Mac` – Indicates the filter is an MAC filter policy.

Label	Description (Continued)
`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 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.

Sample Output

```
===============================================================================
Mac Filter
===============================================================================
Filter Id   : 8                                   Applied        : Yes
Scope       : Template                            Def. Action    : Forward
Entries     : 2
Description : Description for Mac Filter Policy id # 8
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
-------------------------------------------------------------------------------
Entry       : 8                                   FrameType      : Ethernet
Ing. Matches: 80 pkts
Egr. Matches: 62 pkts

Entry       : 10                                  FrameType      : Ethernet
Ing. Matches: 80 pkts
Egr. Matches: 80 pkts
```

Clear Commands

ip

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

Context clear>filter

Description Clears the counters associated with the IP filter policy.

By default, all counters associated with the filter policy entries are reset. The scope of which counters are cleared can be narrowed using the command line parameters.

Default clears all counters associated with the IP filter policy entries.

Parameters *ip-filter-id* — The IP filter policy ID.

Values 1 — 65535

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

Values 1 — 65535

ingress — Specifies to only clear the ingress counters.

egress — Specifies to only clear the egress counters.

ipv6

Syntax **ipv6** *ip-filter-id* **[entry entry-id] [ingress | egress]**

Context clear>filter

Description 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 *ip-filter-id* — The IP filter policy ID.

Values 1 — 65535

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

Values 1 — 65535

ingress — Specifies to only clear the ingress counters.

egress — Specifies to only clear the egress counters.

mac

Syntax **mac** *mac-filter-id* [**entry** *entry-id*] [**ingress | egress**]

Context clear>filter

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.

Values 1 — 65535

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

Values 1 — 65535

ingress — Specifies to only clear the ingress counters.

egress — Specifies to only clear the egress counters.

Monitor Commands

filterip

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

Context monitor

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

Parameters *ip-filter-id* — The IP filter policy ID.

Values 1 — 65535

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

Values 1 — 65535

interval — Configures the interval for each display in seconds.

Default 10 seconds

Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

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

rate — When the **rate** keyword is specified, the rate-per-second for each statistic is displayed instead of the delta.

ipv6

Syntax **ipv6** *ip-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 *ip-filter-id* — The IP filter policy ID.

Values 1 — 65535

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

Values 1 — 65535

interval — Configures the interval for each display in seconds.

Default 10 seconds

Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

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

rate — When the **rate** keyword is specified, the rate-per-second for each statistic is displayed instead of the delta.

mac

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

Context monitor>filter

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

Parameters *mac-filter-id* — The MAC filter policy ID.

Values 1 — 65535

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

Values 1 — 65535

interval — Configures the interval for each display in seconds.

Default 5 seconds

Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

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

rate — When the **rate** keyword is specified, the rate-per-second for each statistic is displayed instead of the delta.

Common CLI Command Descriptions

In This Chapter

This section provides information about common Command Line Interface (CLI) syntax and command usage.

Topics in this chapter include:

Common Service Commands

sap

Syntax [**no**] **sap** *sap-id*

Description This command specifies the physical port identifier portion of the SAP definition.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

The *sap-id* can be configured in one of the following formats:

Type	Syntax	Example
port-id	*slot*/*mda*/*port*[.*channel*]	1/1/5
null	[*port-id* | *lag-id*]	*port-id*: 1/1/3 *lag-id*: lag-3
dot1q	[*port-id* | *lag-id*]:qtag1	*port-id*:qtag1: 1/1/3:100 *lag-id*:lag-1:102

qtag1, qtag2 — Specifies the encapsulation value used to identify the SAP on the port or sub-port. If this parameter is not specificially defined, the default value is 0.

Values qtag1: * | 0 — 4094
qtag2 : * | 0 — 4094

The values depends on the encapsulation type configured for the interface. The following table describes the allowed values for the port and encapsulation types.

Port Type	Encap-Type	Allowed Values	Comments
Ethernet	Null	0	The SAP is identified by the port.
Ethernet	Dot1q	0 — 4094	The SAP is identified by the 802.1Q tag on the port. Note that a 0 qtag1 value also accepts untagged packets on the dot1q port.

Standards and Protocol Support

Standards Compliance

IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery
IEEE 802.1D Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1s Multiple Spanning Tree
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1X Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ah Provider Backbone Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ae 10Gbps Ethernet
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks draft-ietf-disman-alarm-mib-04.txt IANA-IFType-MIB
IEEE8023-LAG-MIB ITU-T G.8032 Ethernet Ring Protection Switching (version 2)

Protocol Support

BGP

RFC 1397 BGP Default Route Advertisement
RFC 1772 Application of BGP in the Internet
RFC 1997 BGP Communities Attribute
RFC 2385 Protection of BGP Sessions via MD5
RFC 2439 BGP Route Flap Dampening
RFC 2547 bis BGP/MPLS VPNs draft-ietf-idr-rfc2858bis-09.txt.
RFC 2918 Route Refresh Capability for BGP-4
RFC 3107 Carrying Label Information in BGP-4
RFC 3392 Capabilities Advertisement with BGP4
RFC 4271 BGP-4 (previously RFC 1771)
RFC 4360 BGP Extended Communities Attribute
RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)(previously RFC 2547bis BGP/MPLS VPNs)
RFC 4760 Multi-protocol Extensions for BGP
RFC 4893 BGP Support for Four-octet AS Number Space

CIRCUIT EMULATION

RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks

DHCP

RFC 2131 Dynamic Host Configuration Protocol (REV)

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
RFC 2697 A Single Rate Three Color Marker
RFC 2698 A Two Rate Three Color Marker
RFC 4115 A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic

IPv6

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2462 IPv6 Stateless Address Auto configuration
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 2740 OSPF for IPv6
RFC 3587 IPv6 Global Unicast Address Format
RFC 4007 IPv6 Scoped Address Architecture
RFC 4193 Unique Local IPv6 Unicast Addresses
RFC 4291 IPv6 Addressing Architecture
RFC 4552 Authentication/Confidentiality for OSPFv3
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
draft-ietf-isis-ipv6-05
draft-ietf-isis-wg-multi-topology-xx.txt

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 (ISIS) 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 3847 Restart Signaling for IS-IS – GR helper

MPLS - LDP

RFC 3037 LDP Applicability
RFC 3478 Graceful Restart Mechanism for LDP — GR helper
RFC 5036 LDP Specification
RFC 5283 LDP extension for Inter-Area LSP
RFC 5443 LDP IGP Synchronization

MPLS - General

RFC 3031 MPLS Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL

Multicast

RFC 1112 Host Extensions for IP Multicasting (Snooping)
RFC 2236 Internet Group Management Protocol, (Snooping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snooping) [Only in 7210 SAS-M access-uplink mode]

NETWORK MANAGEMENT

ITU-T X.721: Information technology- OSI-Structure of Management Information
ITU-T X.734: Information technology- OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
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-BASEDSMMIB
RFC 2575 SNMP-VIEW-BASEDACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MI
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 - Simple Network Management Protocol (SNMP) Applications
RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 - SNMP MIB
draft-ietf-mpls-lsr-mib-06.txt
draft-ietf-mpls-te-mib-04.txt
draft-ietf-mpls-ldp-mib-07.txt

OSPF

RFC 1765 OSPF Database Overflow
RFC 2328 OSPF Version 2
RFC 2370 Opaque LSA Support
RFC 3101 OSPF NSSA Option
RFC 3137 OSPF Stub Router Advertisement
RFC 3623 Graceful OSPF Restart – GR helper
RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2

MPLS - RSVP-TE

RFC 2430 A Provider Architecture DiffServ & TE
RFC 2702 Requirements for Traffic Engineering over MPLS
RFC2747 RSVP Cryptographic Authentication
RFC3097 RSVP Cryptographic Authentication
RFC 3209 Extensions to RSVP for Tunnels
RFC 4090 Fast reroute Extensions to RSVP-TE for LSP Tunnels
RFC 5817 Graceful Shutdown in MPLS and GMPLS Traffic Engineering Networks

PSEUDO-WIRE

RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)
RFC 4446 IANA Allocations for PWE3
RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)
RFC 5085, Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
RFC 5659 An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge
RFC6073, Segmented Pseudowire (draft-ietf-pwe3-segmented-pw-18.txt)
draft-ietf-l2vpn-vpws-iw-oam-02.txt
OAM Procedures for VPWS Interworking
draft-ietf-pwe3-oam-msg-map-14-txt, Pseudowire (PW) OAM Message Mapping
Pseudowire Preferential Forwarding Status bit definition
draft-pwe3-redundancy-02.txt
Pseudowire (PW) Redundancy

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh- newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

TCP/IP

RFC 768 UDP
RFC 1350 The TFTP Protocol
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1519 CIDR
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Interval and Transfer Size option

Timing

ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008
ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.
GR-1244-CORE Clocks for the Synchronized Network: Common Generic Criteria, Issue 3,May 2005
ITU-T G.8261 Telecommunication Standardization Section of ITU, Timing and synchronization aspects in packet networks, issued 04/2008.
ITU-T G.8262 Telecommunication Standardization Section of ITU, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007.
ITU-T G.8264 Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008.
IEEE Std 1588™-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

VPLS

RFC 4762 Virtual Private LAN Services Using LDP (previously draft-ietf-l2vpn-vpls-ldp-08.txt)

VRRP

RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768 Virtual Router Redundancy Protocol

Proprietary MIBs

ALCATEL-IGMP-SNOOPING-MIB.mib
TIMETRA-CAPABILITY-7210-SAS-M-V5v0.mib
(7210 SAS-M Only)
TIMETRA-CAPABILITY-7210-SAS-X-V5v0.mib (7210 SAS-X Only)
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-DOT3-OAM-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IEEE8021-CFM-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-NTP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-SAS-ALARM-INPUT-MIB.mib
TIMETRA-SAS-FILTER-MIB.mib
TIMETRA-SAS-IEEE8021-CFM-MIB.mib
TIMETRA-SAS-IEEE8021-PAE-MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-LOG-MIB.mib.mib
TIMETRA-SAS-MIRROR-MIB.mib
TIMETRA-SAS-MPOINT-MGMT-MIB.mib (Only for 7210 SAS-X)
TIMETRA-SAS-PORT-MIB.mib
TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SDP-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SAS-SERV-MIB.mib
TIMETRA-SAS-VRTR-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-ISIS-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-VRRP-MIB.mib
TIMETRA-VRTR-MIB.mib

INDEX