Alcatel-Lucent

Service Access Switch| Release 8.0 Rev.04

7210 SAS D, E, K OS
Router Configuration Guide

3HE10393AAACTQZZA

Alcatel·Lucent

Disclaimers

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

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

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

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

TABLE OF CONTENTS

LIST OF TABLES

List of 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 D, E, K OS and presents configuration and implementation examples.

On 7210 SAS devices, not all the CLI commands are supported on all the platforms and in all the modes. In many cases, the CLI commands are mentioned explicitly in this document. In other cases, it is implied and easy to know the CLIs that are not supported on a particular platform.

NOTE: 7210 SAS-E and 7210 SAS-D operate in access-uplink mode by default. No explicit user configuration is needed for this.

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
- Virtual routers
- IP and MAC-based filters

List of Technical Publications

The 7210-SAS D, E, K OS documentation set is composed of the following books:

- 7210-SAS D, E, K OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.

- 7210-SAS D, E, K OS System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.

- 7210-SAS D, E, K OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), link aggregation group (LAG) and port provisioning.

- 7210-SAS D, E, K OS Router Configuration Guide

  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, as well as IP and MAC-based filtering.

- 7210-SAS D, E, K OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for routing protocols and route policies.

- 7210-SAS D, E, K OS Services Guide

  This guide describes how to configure service parameters such as customer information, and user services.

- 7210-SAS D, E, K 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 D, E, K OS Quality of Service Guide

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

Technical Support

If you purchased a service agreement for your 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://www.alcatel-lucent.com/wps/portal/support

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 and addresses and router IDs.	IP Router Configuration on page 15
	IP and MAC filters	Filter Policies on page 83
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 339

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 device, 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 following router features can be configured:

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).

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 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.

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.

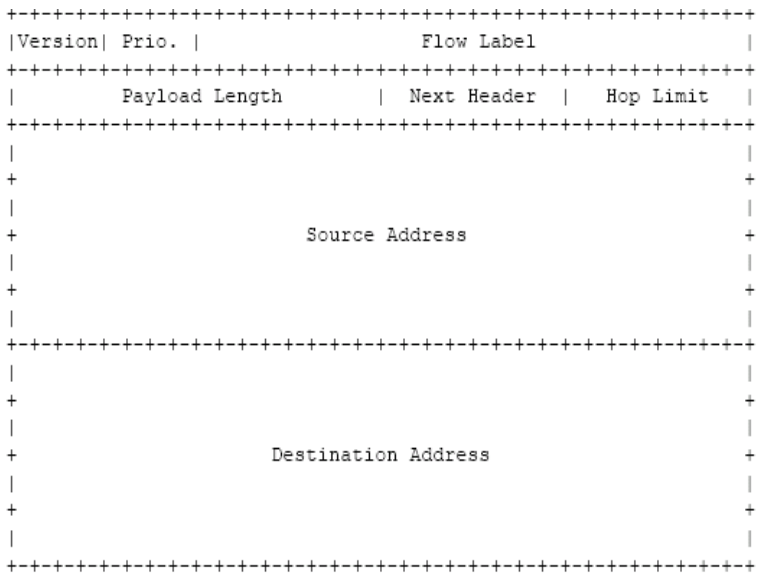


Figure 1: IPv6 Header Format

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 for 7210 SAS-D

The IPv6 applications for 7210 SAS-D are:

- IPv6 inband management of the node using access-uplink port IPv6 IP interface
- IPv6 transit management traffic (using access-uplink port 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.

BFD support on 7210 SAS platforms

BFD in a VPRN service can be used for:

- OSPV2 PE-CE routing protocol
- Static routes (only IPv4)
- VRRP (IPv4)

BFD in IES service can be used for:

- OSPFv2
- IS-IS for IPv4 interfaces
- Static routes (only IPv4)
- VRRP (IPv4)

BFD in Base routing instance can be used for:

- OSPFv2 on network IPv4 interfaces
- IS-IS on network IPv4 interfaces
- MP-BGP for vpn-ipv4 and vpn-ipv6 family (only multi-hop)
- Static routes (only IPv4)
- RSVP-TE
- PIM (IPv4)

Process Overview

The following items are components to configure basic router parameters.

- 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)

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.

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 system or a loopback interface.

A system interface should be configured.

System Interface

The system interface is associated with the network entity , not a specific interface.

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.

Basic Configuration

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
...
     exit
     exit
...
#------------------------------------------
A:ALA-A> config#
```

Common Configuration Tasks

The following sections describe basic system tasks.

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 IP interface. The system interface assigns an IP address to the interface in the IES context and create logical IP interfaces for inband management.

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]}
```

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#
```

- is sprayed "*configure>system>resource-profile>router>ecmp <max-ecmp-routes>*" and on7210 SAS-R6 and R12 it is "*configure>system>global-resource-profile>router>ecmp <max-ecmp-routes>*For more information about the resource profile command, see the “7210 SAS M,T,X,R6, R12, Mxp Basic System Configuration User Guide”.
- LDP LER ECMP (including LDP over RSVP) is not supported. LDP LSR ECMP is supported on certain platforms. Check the release notes and the 7210 SAS MPLS guide to know the platforms that support it and to learn more about it. IPv4 ECMP and LDP LSR ECMP share common set of resources in the hardware. Refer the 7210 SAS System Basic guide to learn about resource allocation for IPv4 ECMP and LDP LSR ECMP.

Service Management Tasks

This section discusses the following service management tasks:

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#
```

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

config

— **router** [*router-name*]
- — **[no] static-route {***ip-prefix/prefix-length* | *ip-prefix netmask***}[preference** *preference***] [metric** *metric***] [enable | disable] next-hop** *ip-address*
- — **[no] static-route {***ip-prefix/prefix-length* | *ip-prefix netmask***} [preference** *preference***] [metric** *metric***] [enable | disable] black-hole**
- — **interface** *interface-name*
- — **no interface** *interface-name*

Router Interface Commands

config
- **router** [*router-name*]
  - [**no**] **interface** *ip-int-name* **[unnumbered-mpls-tp]**
    - **address** {*ip-address/mask* | *ip-address netmask*} [**broadcast** {**all-ones** | **host-ones**}]
    - **no address**
    - **delayed-enable**
    - **no delayed-enable**
    - **description** *long-description-string*
    - **no description**
    - **icmp**
      - **redirects** [*number seconds*]
      - **no redirects**
      - **ttl-expired** [*number seconds*]
      - **no ttl-expired**
      - **unreachables** [*number seconds*]
      - **no unreachables**
    - [**no**] **loopback**
    - [**no**] **shutdown**

Router Interface IPv6 Commands (supported only on 7210 SAS-D)

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**
      - **link-local-address** *ipv6-address* **[preferred]**
      - [**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**

Show Commands

show
- **router** *router-instance*
  - **arp** [*ip-int-name* | *ip-address/mask* | **mac** *ieee-mac-address* | **summary**] [**local** | **dynamic** | **static]**
  - **dhcp**
    - **statistics [interface** *ip-int-name*|*ip-address***]**
    - **summary**
  - **interface** [{[*ip-address* | *ip-int-name*] [**detail**]} | [**summary**]
  - **interface** [*ip-address* | *ip-int-name*] [**detail**]
  - **interface** [*ip-address* | *ip-int-name*]
  - **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**] **[dynamic|static|managed]**
  - **route-table** [*ip-address*[mask] [longer|exact]]|[**summary]**
  - **route-table** [*family*] [**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*| **tag** *tag*] | [**detail**]
  - **status**

Clear Commands

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

Debug Commands

debug
- **trace**
- **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

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.

static-route

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

[**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.

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.

ipv4-address a.b.c.d (host bits must be 0)*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 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 multiple routes are learned with an identical preference using the same protocol, the lowest- cost route is used. **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 routes with different preferences then the lower preference route will be installed.
- 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 the same preference and metric, then the route with the lowest next-hop IP address will be installed.

Default 1

Values 0 — 65535

next-hop *ip-address* **—** Specifies the directly connected next hop IP address used to reach the destination.

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 *ip-address* 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

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

Router Interface Commands

interface

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

Context config>router

Description This command creates a system or a loopback IP routing interface. Once created, attributes like IP address, 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 , 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 addressto a system IP interface. Only one IP address can be associated with an IP interface.

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.

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**

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

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.

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

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.

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.

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.

.

Show Commands

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.
Int	The ARP entry is an internal ARP entry.
[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
===============================================================================
```

neighbor

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

Context show>router

Description This command displays information about the IPv6 neighbor cache.

Parameters *ip-int-name* — 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.

dynamic — The Ipv6 neighbor entry is a dynamic neighbor entry.

static — The Ipv6 neighbor entry is an active static neighbor entry.

managed — The Ipv6 neighbor entry is a managed neighbor entry.

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.

Label	Description (Continued)
Interface	Displays the interface name.
Rtr	Specifies whether a neighbor is a router.
Dynamic	The Ipv6 neighbor entry is a dynamic neighbor entry.
Static	The Ipv6 neighbor entry is an active static neighbor entry.
Managed	The Ipv6 neighbor entry is a managed neighbor entry.
Mtu	Displays the MTU size.

Sample Output

```
*A:Dut-A>config>router# show router neighbor

===============================================================================
Neighbor Table (Router: Base)
===============================================================================
IPv6 Address                                Interface
   MAC Address                State         Expiry          Type         RTR
-------------------------------------------------------------------------------
2193:12:17:1::5                             A_to_B2_17
   00:00:1b:00:00:01          REACHABLE     -               Static       No
2193:12:23:1::2                             A_to_B2_23
   e4:81:84:24:1d:6c          STALE         01h12m35s       Dynamic      Yes
-------------------------------------------------------------------------------
No. of Neighbor Entries: 2
===============================================================================
*A:Dut-A>config>router# show router neighbor dynamic

===============================================================================
Neighbor Table (Router: Base)
===============================================================================
IPv6 Address                                Interface
   MAC Address                State         Expiry          Type         RTR
-------------------------------------------------------------------------------
2193:12:23:1::2                             A_to_B2_23
   e4:81:84:24:1d:6c          STALE         01h12m27s       Dynamic      Yes
-------------------------------------------------------------------------------
No. of Neighbor Entries: 1
===============================================================================
*A:Dut-A>config>router#
*A:Dut-A>config>router# show router neighbor static

===============================================================================
Neighbor Table (Router: Base)
===============================================================================
IPv6 Address                                Interface
   MAC Address                State         Expiry          Type         RTR
-------------------------------------------------------------------------------
2193:12:17:1::5                             A_to_B2_17
   00:00:1b:00:00:01          REACHABLE     -               Static       No
-------------------------------------------------------------------------------
No. of Neighbor Entries: 1
```

```
===============================================================================
*A:Dut-A>config>router# show router neighbor ma
mac      managed
*A:Dut-A>config>router# show router neighbor managed

===============================================================================
Neighbor Table (Router: Base)
===============================================================================
IPv6 Address                                 Interface
   MAC Address               State         Expiry          Type         RTR
```

dhcp

Syntax **dhcp**

Context show>router

Description This command enables the context to display DHCP information for the specified service.

statistics

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

Context show>router>dhcp

Description Displays DHCP statistics information.

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

Show DHCP Statistics Output — The following table describes the output fields for DHCP statistics.

Label	Description
Received Packets	The number of packets received from the DHCP clients. Includes DHCP packets received from both DHCP client and DHCP server.
Transmitted Packets	The number of packets transmitted to the DHCP clients. Includes DHCP packets transmitted from both DHCP client and DHCP server.
Received Malformed Packets	The number of corrupted/invalid packets received from the DHCP clients. Includes DHCP packets received from both DHCP client and DHCP server
Received Untrusted Packets	The number of untrusted packets received from the DHCP clients. In this case, a frame is dropped due to the client sending a DHCP packet with Option 82 filled in before “trust” is set under the DHCP interface command.
Client Packets Discarded	The number of packets received from the DHCP clients that were discarded.
Client Packets Relayed	The number of packets received from the DHCP clients that were forwarded.
Client Packets Snooped	The number of packets received from the DHCP clients that were snooped.
Server Packets Discarded	The number of packets received from the DHCP server that were discarded.

Label	Description
Server Packets Relayed	The number of packets received from the DHCP server that were forwarded.
Server Packets Snooped	The number of packets received from the DHCP server that were snooped.

```
*A:7210SAS>show>router>dhcp# statistics

===============================================================
DHCP Global Statistics, service 1
===============================================================
Rx Packets                          : 416554
Tx Packets                          : 206405
Rx Malformed Packets                : 0
Rx Untrusted Packets                : 0
Client Packets Discarded            : 0
Client Packets Relayed              : 221099
Client Packets Snooped              : 0
Client Packets Proxied (RADIUS)     : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Discarded            : 0
Server Packets Relayed              : 195455
Server Packets Snooped              : 0
DHCP RELEASEs Spoofed               : 0
DHCP FORCERENEWs Spoofed            : 0
===============================================================
*A:7210SAS>show>service>id>dhcp#
```

summary

Syntax **summary**

Context show>router>dhcp

Description Displays DHCP configuration summary information.

Output **Show DHCP Summary Output —** The following table describes the output fields for DHCP summary.

Label	Description
Interface Name	Name of the router interface.
Arp Populate	Specifies whether or not ARP populate is enabled. 7210 SAS does not support ARP populate.
Used/Provided	7210 SAS does not maintain lease state.
Info Option	Indicates whether Option 82 processing is enabled on the interface.
Admin State	Indicates the administrative state.

Sample Output

```
A:7210SAS# show router dhcp summary
DHCP Summary, service 1
===============================================================================

Interface Name                   Arp      Used/                Info    Admin
  SapId/Sdp                      Populate Provided             Option  State
-------------------------------------------------------------------------------
egr_1                            No       0/0                  Replace Up
i_1                              No       0/0                  Replace Up
-------------------------------------------------------------------------------
Interfaces: 2
===============================================================================

*A:7210SAS>show>service>id>dhcp#
```

fib

Syntax

Context show>router

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

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

ipv4-prefix: a.b.c.d (host bits must be 0)
ipv4-prefix-length: 0 — 32**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**]}
interface [{[*ip-address* | *ip-int-name*] [**detail**] [*family*]} | [**summary**] | [**exclude-services**]
interface *family* [**detail**]
interface [*ip-address* | *ip-int-name*]

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

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

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

detail — Displays detailed IP interface information.

family — Specifies the router IP interface family to display.

Values **ipv4** — Displays the peers that are IPv6-capable.
ipv6 — Displays the peers that are IPv6-capable.

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#
A:ALA-A# show router interface 6.6.6.2
===============================================================================
Interface Table (Router: Base)
===============================================================================
Interface-Name             Adm         Opr         Mode    Port/SapId
   IP-Address                                                PfxState
-------------------------------------------------------------------------------
to-PE-E                    Up          Up           IES     1/1/3:0.*
   6.6.6.2/24                                                n/a
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
A:ALA-A#
```

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.

Label	Description (Continued)
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.

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: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

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

route-table

Syntax **route-table [*ip-address*[mask] [longer|exact]]|[summary]**

Context show>router

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

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

Parameters *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.
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.

```
A:ALA# show router route-table
===============================================================================
Route Table (Router: Base)
===============================================================================
```

```
Dest Prefix                          Type        Proto      Age          Pref
       Next Hop[Interface Name]                                      Metric
-------------------------------------------------------------------------------
1.1.1.1/32                           Remote      Static     00h22m29s    5
       6.6.6.1                                                             1
2.2.2.2/32                           Local       Local      00h22m52s    0
       system                                                              0
5.5.5.0/24                           Remote      Static     00h22m29s    5
       6.6.6.1                                                             1
6.6.6.0/24                           Local       Local      00h22m30s    0
       to-PE-E                                                             0
-------------------------------------------------------------------------------
No. of Routes: 4
===============================================================================
A:ALA#

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                         7                       7
===============================================================================
A:ALA-A#
```

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 Imask*] | [**preference** *preference*] | [**next-hop** *ip-address*| **tag** *tag*]

Context show>router

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

Parameters

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

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

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

Values 1 — 4294967295

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.
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. 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.
Max Routes	The maximum number of routes configured for the system.
Total Routes	The total number of routes in the route table.

Sample Output

```
A:DUT-B>show>router# show router status
===============================================================
Router Status (Router: Base)
===============================================================
                         Admin State         Oper State
---------------------------------------------------------------
Router                   Up                  Up
```

```
Max Routes               10000
Total IPv4 Routes        5
ECMP Max Routes          1
===============================================================
A:DUT-B>show>router#
```

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 *service-id*:1 — 2147483647

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.

dhcp

Syntax **dhcp**

Context clear>router

Description This command enables the context to clear DHCP related information.

statistics

Syntax **statistics [ip-address | ip-int-name]**

Context clear>router>dhcp

Description This command clear statistics for DHCP relay and snooping statistics.

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

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

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

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 *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)
* — 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*.

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 access uplink ports to control network traffic into (ingress) or out of (egress) a service access port (SAP) or access uplink 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 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 criteriaand also an action to be taken upon a match.

In 7210 SAS-D and 7210 SAS-E, the available ingress and egress (egress CAM resources allocation is supported only on 7210 SAS-D) 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: IES IP interface in access-uplink mode in 7210 SAS-D) 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 -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 tables below provides more details on use of filter policies.

Table 3:

Table 4:

Table 5: Applying Filter Policies for 7210 SAS-D and 7210 SAS-K

Service	IPv4 Filter	IPv6 filter	MAC Filter
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)
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)
RVPLS (VPLS SAPs)	VPLS access (ingress and egress) and access-uplink SAPs (ingress and egress)	Not Available	Not Available
RVPLS (RVPLS IES IP Interface)	Ingress Override filters (ingress)	Not Available	Not Available
IES	IES access SAP, IES access-uplink SAP	IES access-uplink SAP	Not Available

Table 6: Applying Filter Policies for 7210 SAS-E

Service	IPv4 Filter	IPv6 filter	MAC Filter
Epipe	Epipe access SAP (egress and ingress), Epipe access-uplink SAP (egress and ingress)	Epipe access SAP (ingress only), Epipe access-uplink SAP (ingress only)	Epipe (egress and ingress), Epipe access-uplink SAP (egress and ingress)
VPLS	VPLS access SAP (ingress and egress), VPLS access-uplink SAP (ingress and egress)	VPLS access SAP (ingress only), VPLS access-uplink SAP (ingress only)	VPLS access SAP (ingress and egress), VPLS access-uplink SAP (ingress and egress)
VPLS (RVPLS SAPs)	Routed VPLS is not supported	Routed VPLS is not supported	Routed VPLS is not supported
IES	Ingress and egress of IES access SAP and IES access-uplink SAP	Not Available	Not Available

ACL on range SAPs

The ACLs on VLAN range SAPs are supported only on ingress (for Epipe and VPLS services).

.

Table 8: Applying ACLs support on Epipe and VPLS services on 7210 SAS-D and 7210 SAS-K variants when using range SAPs

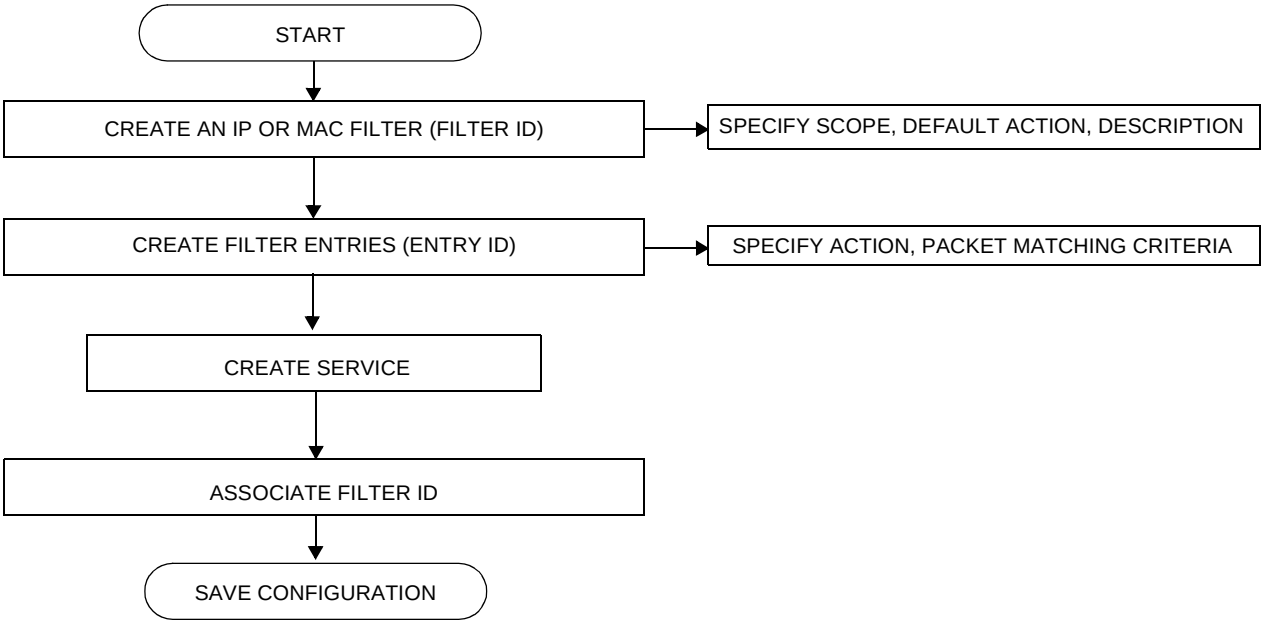
Types of filters	Epipe	VPLS
Ingress IP or IPv6	Yes	Yes
Ingress MAC	Yes	Yes
Egress IP	No	No
Egress MAC	No	No

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 ingress policies can be applied on SAP created on access ports or access uplink ports.
- 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. SAP egress policies can be applied on both access ports and access uplink ports.
- IES IP interfaces — IP filter policies are applied to IES SAPs (ingress and egress).

NOTE: For details on filter support for various services and SAPs on different platforms, see “Table 5, “Applying Filter Policies for 7210 SAS-D and 7210 SAS-K,”Table 6, “Applying Filter Policies for 7210 SAS-E,”Table 7, “Applying Filter Policies for 7210 SAS-K,”.

Creating and Applying Policies



Packet Matching Criteria

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 .
- DSCP marking — Entering a DSCP marking enables the filter to search for the DSCP marking specified in this field. See Table 10, DSCP Name to DSCP Value Table, on page 94.
- 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. This is not supported on 7210 SAS-K devices.

- 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.

-

- Outer Dot1p (Only on 7210 SAS-K)

  Entering the Outer Dot1p value or range (using the mask) allows the filter to search for frames whose outermost Dot1p (that is, the Dot1p in the outermost VLAN tag of the packet) matches the Dot1p value configured. The Dot1p value and mask accepts decimal values in the range 0 to 7.

- Inner Outer Dot1p (Only on 7210 SAS-K)

  Entering the Inner Dot1p value or range (using the mask) allows the filter to search for frames whose inner Dot1p (thats is, the Dot1p in the VLAN tag immediately following the

outermost VLAN tag of the packet) matches the Dot1p value configured. The Dot1p value and mask accepts decimal values in the range 0 to 7.

DSCP Values

Table 9: 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 9: 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 2 displays an example of several packets forwarded upon matching the filter criteria and several packets traversing through the filter entries and then dropped.

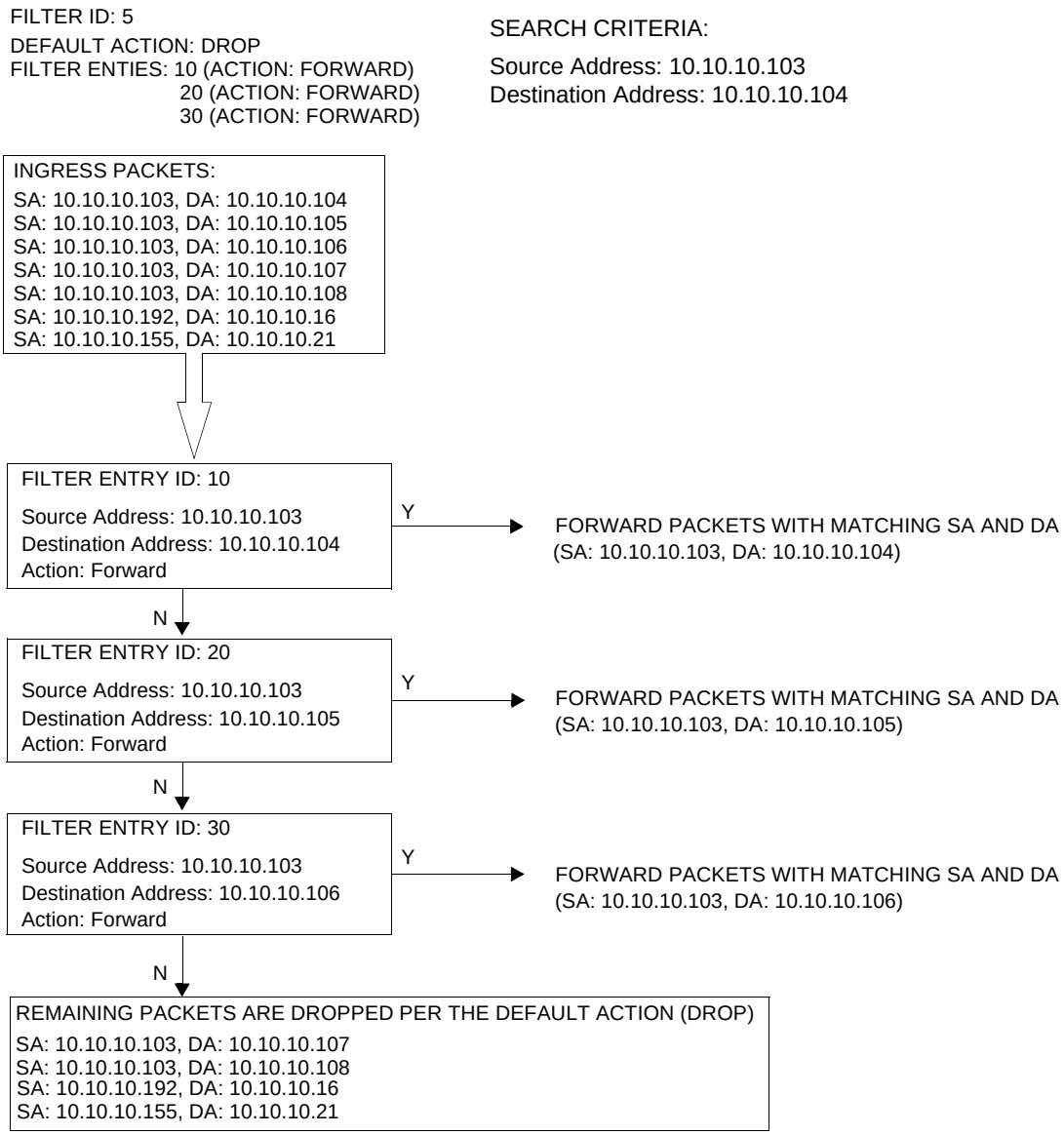


Figure 2: Filtering Process Example

Applying Filters

After filters are created, they can be applied to the following entities:

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 an IES Interface

An IP filter can be applied an IES SAP. 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.
- IP filters applied on an IES SAP cannot match against IP packets containing IP options.
- 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. Ingress filter CAM resources used to match packet fields are shared with other features such as SAP ingress QoS, CFM UP MEP, and G8032. By default software assigns a fixed amount of resources for use by ingress ACLs. User has an option to either increase this by taking away resources from other features or decrease by taking away resources from ingress ACLs. The number of ACLs that can be supported is directly depdendent on the amount of resources allocated towards ingress ACLs.
- In 7210 SAS-D and SAS-E, 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.
- In 7210 SAS-D and SAS-E, 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.In 7210 SAS-D and SAS-E, 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.
- In 7210 SAS-D, 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).

- In 7210 SAS-D, 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). In 7210 SAS-E, the available egress CAM hardware resources are allocated equally among IP match criteria and MAC criteria on system bootup.
- In 7210 SAS-D and SAS-E, IPv6 ACLs and MAC QoS policies cannot co-exist on the SAP.
- In 7210 SAS-D and SAS-E, 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.
- Only 7210 SAS-K allows for use of outer VLAN ID and inner VLAN ID for match in MAC criteira with both ingress and egress ACLs. Other 7210 SAS platforms do not support use of outer and inner VLAN ID field for match in the MAC criteria.

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 10: MAC Match Criteria Exclusivity Rules

Frame Format	Etype
Ethernet – II	Yes
802.3	No
802.3 – snap	No
802.3-llc	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 for 7210 SAS-D and SAS-E

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 fixed-size entries (example - 256 entries per chunk on 7210 SAS-D). 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. An ipv6 128 bit address uses 2 entries from the chunk for every match entry configured in filter policy, whereas, an IP filter uses only one entry from the chunk for every entry configured.
- **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 (supported only for 7210 SAS-D)

Note: 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 128

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 256 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 250 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 128 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.

Resource Usage for Ingress Filter Policies for 7210 SAS-K

When the user allocates resources from the ingress CAM resource pool for use by filter policies using the *configure> system> resource-profile> ingress-internal-tcam> acl-sap-ingress* CLI commands, the system allocates resources in chunks of fixed-size entries (512 entries per chunk on 7210 SAS-K). Resources must be allocated using these commands before associating a filter policy with the SAP, else software will error out the command. The usage of these entries by different type of match criteria is given below:

- mac-criteria, ipv4-criteria and ipv6-criteria with 64-bit-address:

User needs to allocate resources, in terms of number of slices, for filter policies that use mac criteria, ipv4 criteria and ipv6 64-bit criteria from the ingress internal tcam resource pool using the command "*configure> system> resource-profile> ingress-internal-tcam> acl-sap-ingress"*. The entries allocated are shared by filter policies that use any of these criteria. Each filter entry configured in the policy takes away a single resource from the pool allocated for filter policies.

- ipv6-criteria with 128-bit address:

User needs to allocate resources, in terms of number of slices, for filter policies that use ipv6 128-bit criteria from the ingress internal tcam resource pool using the command "*configure> system> resource-profile> ingress-internal-tcam> acl-sap-ingress>mac-ipv4-ipv6-128-match-enable*". User can allocate all the slices allocated for the filter policies (using the command *configure> system> resource-profile> ingress-internal-tcam> acl-sap-ingress*) for use by ipv6 criteria with 128-bit addresses or allocation only a portion of it. The entries allocated are used by filter policies that use ipv6 criteria with 128-bit addresses. Each filter entry configured in the policy takes away

two (2) resources from the pool. Software uses these resources also for mac criteria, ipv4 criteria, and ipv6 crteria with 64-bit address. Irrespective of the criteria, two (2) resources are taken for each entry configured on the filter policy.

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-D:

```
*A:SASD>config>system>res-prof>ing-internal-tcam# info detail
----------------------------------------------
                acl-sap-ingress 2
                    ipv4-match-enable max
                    no ipv6-64-only-match-enable
                    no ipv4-ipv6-128-match-enable
                    mac-match-enable 2
                exit
                no eth-cfm
----------------------------------------------
*A:SASD>config>system>res-prof>ing-internal-tcam# acl-sap-ingress
```

The following example displays a sample configuration of allocation of egress internal CAM resources for egress policy for 7210 SAS-D:

```
A:SASD>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:SASD>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 3 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 figure shows the IP filter applied to an ingress interface.

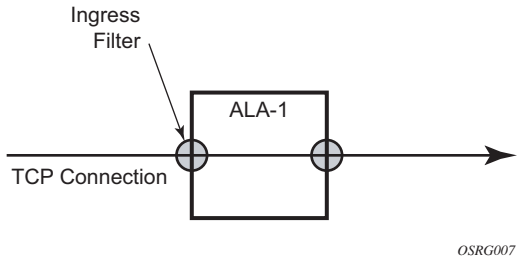


Figure 3: Applying an IP Filter to an Ingress Interface

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 110
- Creating a MAC Filter Policy on page 115
- Filter policies can be associated with the following entities: on page 88

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
- 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 (applicable only for 7210 SAS-D)

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 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 Filter Policies to an IES Interface

IP filter policies can be applied to an IP interface created in an IES service. These filter policies apply to the routed management traffic.

CLI Syntax:
```
config>service>ies# interface ip-int-name
    address ip-address
    sap sap-id
       ingress
          filter ip ip-filter-id
```

The following displays an IP filter applied to an IES sap at ingress.

```
A:ALA-48>config>service>ies# info
----------------------------------------------
            interface "to-104" create
                address 10.1.2.1/24
                sap lag-2:0.* create
                      ingress
                            filter ip 10
                exit
            exit
...
----------------------------------------------
A:ALA-48>config>service>ies#
```

Filter Management Tasks

This section discusses the following filter policy management tasks:

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 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#
```

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 124
- From an Egress SAP on page 124
- From the Filter Configuration on page 125

From an Ingress SAP

To remove a filter from an ingress SAP, enter the following CLI commands:

CLI Syntax:
```
config>service# [epipe | ies | 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 | ies | 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 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
            — filter-name filter-name
            — no filter-name
            — 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
                    — 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
            — filter-name filter-name
            — no filter-name
            — entry entry-id  [time-range time-range-name] [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}
                    — no dst-ip
                    — 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 for 7210 SAS-D and 7210 SAS-E

```
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
            — filter-name filter-name
            — no filter-name
            — renum old-entry-id new-entry-id
            — scope {exclusive | template}
            — no scope
            — type filter-type
```

MAC Filter Policy Commands for 7210 SAS-K

```
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
                    — dst-mac ieee-address [ieee-address-mask]
                    — no dst-mac
                    — etype 0x0600..0xffff
                    — no etype
                    — inner-dot1p dot1p-value [dot1p-mask]
                    — no inner-dot1p
                    — inner-tag value [vid-mask]
                    — no inner-tag
                    — outer-dot1p dot1p-value [dot1p-mask]
                    — no outer-dot1p
                    — no outer-tag
                    — outer-tag value [vid-mask]
                    — src-mac ieee-address [ieee-address-mask]
                    — no src-mac
            — filter-name filter-name
            — no filter-name
            — renum old-entry-id new-entry-id
            — scope {exclusive | template}
            — no scope
            — type filter-type
```

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 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 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 99, 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 .

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). 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 .

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)

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
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.

ethernet_II — Specifies the frame type is Ethernet Type 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

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 *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 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.

false — Specifies matching on IP packets that do not have any option field present in the IP header.

src-ip

Syntax **src-ip** {*ip-address*[*Imask*]} [*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

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 *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.

Egress Dot1p values used for matching will correspond to the Dot1p values used for remarking.

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)

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	DDDDDDDDDDDDD	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 0xFFFFFF000000

Default **0xFFFFFFFFFFFF (exact match)**

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

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.

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

inner-dot1p

Syntax **inner-tag** *value [vid-mask]*
no inner-tag

Context config>filter>mac-filter>entry>match

Description **Platforms Supported:** 7210 SAS-K.

Configures the Dot1p value to be used to match against the Dot1p value in the inner tag (the one that follows the outermost tag in the packet) of the received packet.

The no form of this command removes the previously entered dot1p value as the match criteria.

Default no inner-dot1p

Parameters *dot1p-value* — Specify the Dot1p value to match.

Values [0..7]

dot1p-mask — Specify the mask value to match a range of Dot1p values.

Values [0..7] - accepts decimal hex or binary

inner-tag

Syntax **inner-tag** *value [vid-mask]*
no inner-tag

Context config>filter>mac-filter>entry>match

Description **Platforms Supported:** 7210 SAS-K.

Configures the VLAN value to be used to match against the VLAN value in the inner tag (the one that follows the outermost tag in the packet) of the received packet.

The optional vid_mask is defaulted to 4095 (exact match) but may be specified to allow pattern matching. The masking operation is ((value & vid-mask) = = (tag & vid-mask)). A value of 6 and a mask of 7 would match all VIDs with the lower 3 bits set to 6.

The no form of this command removes the previously entered VLAN tag value as the match criteria.

Default no inner-tag

Parameters *value* — Specify the VLAN value to use for the match

Values [0..4095] decimal or [0x0..0xFFF] hex

vid-mask — Specify the mask value to match a range of VLAN values.

Values [1..4095] decimal or [0x1..0xFFF] hex

outer-dot1p

Syntax **outer-tag** *value [vid-mask]*
no outer-tag

Context config>filter>mac-filter>entry>match

Description **Platforms Supported:** 7210 SAS-K.

Configures the Dot1p value to be used to match against the Dot1p value in the outermost tag of the received packet.

The no form of this command removes the previously entered dot1p value as the match criteria.

Default no outer-dot1p

Parameters *dot1p-value* — Specify the Dot1p value to match.

Values [0..7]

dot1p-mask — Specify the mask value to match a range of Dot1p values.

Values [0..7] - accepts decimal hex or binary

outer-tag

Syntax **outer-tag** *value [vid-mask]*
no outer-tag

Context config>filter>mac-filter>entry>match

Description **Platforms Supported:** 7210 SAS-K.

Configures the VLAN value to be used to match against the VLAN value in the inner tag (the one that follows the outermost tag in the packet) of the received packet.

The optional vid_mask is defaulted to 4095 (exact match) but may be specified to allow pattern matching. The masking operation is ((value & vid-mask) = = (tag & vid-mask)). A value of 6 and a mask of 7 would match all VIDs with the lower 3 bits set to 6.

The no form of this command removes the previously entered VLAN tag value as the match criteria.

Default no outer-tag

Parameters *value* — Specify the VLAN value to use for the match

Values [0..4095] decimal or [0x0..0xFFF] hex

vid-mask — Specify the mask value to match a range of VLAN values.

Values [1..4095] decimal or [0x1..0xFFF] hex

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	DDDDDDDDDDDDD	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.

filter-name

Syntax **filter-name** *filter-name*

Context config>filter>ip-filter
config>filter>ipv6-filter
config>filter>mac-filter

Description This command configures filter-name attribute of a given filter. filter-name, when configured, can be used instead of filter ID to reference the given policy in the CLI.

Default no filter-name

Parameters *filter-name* — A string of up to 64 characters uniquely identifying this filter policy.

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

type

Syntax **type** *filter-type*

Context config>filter>mac-filter

Description This command configures the type of mac-filter as normal, ISID or VID types.

Default normal

Parameters *filter-type* — Specifies which type of entries this MAC filter can contain.

Values normal — Regular match criteria are allowed; ISID or VID filter match criteria not allowed.
isid — Only ISID match criteria are allowed.
vid — On.y VID match criteria are allowed on ethernet_II frame types.

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           :
 - 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 12: 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 13: 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 13: 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 14: 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 15: 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 15: 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.
Outer Dot1p	The IEEE 802.1p value for the match criteria used to match the Dot1p in the outermost VLAN tag. Undefined indicates no value is specified.
inner Dot1p	The IEEE 802.1p value for the match criteria used to match the Dot1p in the inner VLAN tag. Undefined indicates no value is specified.

Label	Description (Continued)
Outer TagVal	The VLAN ID value for the match criteria used to match the VLAN ID in the outermost VLAN tag. Undefined indicates no value is specified.
Inner TagVal	The IEEE 802.1p value for the match criteria used to match the Dot1p in the inner VLAN tag. Undefined indicates no value is specified.
Ethertype	The Ethertype value match criterion.
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.
(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.

Label	Description (Continued)
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.
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
```

Sample Output for 7210 SAS-K

```
===============================================================================
Mac Filter
===============================================================================
Filter Id   : 1                                 Applied         : No
Scope       : Template                          Def. Action     : Drop
Entries     : 1                                 Type            : unknown
Description : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
```

```
-------------------------------------------------------------------------------
Entry       : 1 (Inactive)
Description : (Not Specified)
Src Mac     :
Dest Mac    :
Outer Dot1p*: none                          Outer Dot1p Mask: none
Inner Dot1p*: none                          Inner Dot1p Mask: none
Outer TagVal: none                          Outer TagMask   : none
Inner TagVal: none                          Inner TagMask   : none
Ethertype   : Undefined
Match action: Drop
Ing. Matches: 0 pkts
Egr. Matches: 0 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 **ip** *ip-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor>filter

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>filter

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
qinq	[*port-id* | *lag-id*]:*qtag1.qtag2*	*port-id*:qtag1.qtag2: 1/1/3:100.10 *lag-id*:qtag1.qtag2:lag-10:

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.
Ethernet	QinQ	qtag1: 0 — 4094 qtag2: 0 — 4094	The SAP is identified by two 802.1Q tags 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 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
IANA-IFType-MIB
IEEE8023-LAG-MIB
ITU-T G.8032 Ethernet Ring Protection Switching (version 2)

Protocol Support

DHCP

RFC 2131 Dynamic Host Configuration Protocol
RFC 3046 DHCP Relay Agent Information Option (Option 82)

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 3140 Per-Hop Behavior Identification Codes
RFC 4115 A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic [Only for 7210 SAS-D]

IPv6 (only 7210 SAS-D and 7210 SAS-E)

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 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 5095 Deprecation of Type 0 Routing Headers in IPv6

Multicast (only 7210 SAS-D and 7210 SAS-E)

RFC 1112 Host Extensions for IP Multicasting (Snooping)
RFC 2236 Internet Group Management Protocol, (Snooping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)

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 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
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-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 Simple Network Management Protocol (SNMP) Applications
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 SNMP MIB draft-ietf-disman-alarm-mib-04.txt
RFC 3418 SNMP MIB

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 (Only on 7210 SAS-D ETR and 7210 SAS-K)

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.

Proprietary MIBs

ALCATEL-IGMP-SNOOPING-MIB.mib

TIMETRA-CAPABILITY-7210-SAS-E-V5v0.mib (Only for 7210 SAS-E)

TIMETRA-CAPABILITY-7210-SAS-D-V5v0.mib (Only for 7210 SAS-D)

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 (only on 7210 SAS-D,E)

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-GLOBAL-MIB.mib

TIMETRA-SAS-LOG-MIB.mib.mib

TIMETRA-SAS-MIRROR-MIB.mib

TIMETRA-SAS-PORT-MIB.mib

TIMETRA-SAS-QOS-MIB.mib

TIMETRA-SAS-SYSTEM-MIB.mib

TIMETRA-SCHEDULER-MIB.mib

TIMETRA-SECURITY-MIB.mib

TIMETRA-SERV-MIB.mib

TIMETRA-SYSTEM-MIB.mib

TIMETRA-TC-MIB.mib

TIMETRA-VRTR-MIB.mib

INDEX

F

I