# Table of Contents

## Preface

- Alcatel-Lucent 7210 SAS-Series Router Configuration Process ........................................... 9

## Getting Started

- Alcatel-Lucent 7210 SAS-Series Router Configuration Process ........................................... 13

## IP Router Configuration

- Configuring IP Router Parameters ................................................................. 16
  - Interfaces ....................................................................................... 16
  - System Interface ........................................................................ 16
  - Process Overview ......................................................................... 17
- Configuration Notes ........................................................................ 18
- Configuring an IP Router with CLI ......................................................... 19
  - Router Configuration Overview ...................................................... 20
- System Interface .............................................................................. 20
- Basic Configuration ........................................................................ 21
- Common Configuration Tasks ............................................................. 22
  - Configuring a System Name .......................................................... 22
  - Configuring Interfaces ................................................................. 23
  - Configuring a System Interface ..................................................... 23
- Service Management Tasks ................................................................. 24
  - Changing the System Name .......................................................... 24
  - Deleting a Logical IP Interface ..................................................... 25
  - IP Router Command Reference ..................................................... 27

## Filter Policies

- Filter Policy Configuration Overview ....................................................... 60
  - Service-Based Filtering .................................................................. 60
  - Filter Policy Entities ..................................................................... 61
  - Applying Filter Policies ............................................................... 61
  - Creating and Applying Policies ....................................................... 62
  - Packet Matching Criteria ............................................................. 64
  - Ordering Filter Entries ................................................................ 68
  - Applying Filters ........................................................................... 70
- Configuration Notes ........................................................................... 71
  - MAC Filters ................................................................................. 72
  - IP Filters ...................................................................................... 73
- Configuring Filter Policies with CLI ...................................................... 75
  - Basic Configuration ...................................................................... 76
- Common Configuration Tasks ............................................................. 77
  - Creating an IP Filter Policy ........................................................... 77
    - IP Filter Policy ........................................................................ 77
    - IP Filter Entry .......................................................................... 78
    - IP Entry Matching Criteria ....................................................... 79
  - Creating a MAC Filter Policy .......................................................... 80
Table of Contents

MAC Filter Policy ................................................................. 80
MAC Filter Entry ................................................................. 81
MAC Entry Matching Criteria ................................................. 82
Applying Filter Policies ......................................................... 83
Apply IP and MAC Filter Policies ........................................... 83
Apply Filter Policies to an IES Interface ................................. 84
Filter Management Tasks ....................................................... 85
Renumbering Filter Policy Entries ......................................... 85
Modifying an IP Filter Policy ................................................. 87
Modifying a MAC Filter Policy .............................................. 89
Deleting a Filter Policy ......................................................... 90
  From an Ingress SAP ......................................................... 90
  From an Egress SAP ......................................................... 90
  From the Filter Configuration ............................................ 91
Copying Filter Policies ........................................................ 92
Filter Command Reference ................................................... 93

Common CLI Command Descriptions
  Common Service Commands ................................................. 134

Standards and Protocol Support ............................................ 135

Index .................................................................................... 137
LIST OF TABLES

Getting Started
Table 1: Configuration Process ................................................................. 13

Filter Policies
Table 2: Applying Filter Policies ................................................................. 61
Table 3: DSCP Name to DSCP Value Table .................................................. 66
Table 4: MAC Match Criteria Exclusivity Rules .......................................... 72
Table 5: Applying Filter Policies ................................................................. 83
LIST OF FIGURES

Filter Policies
Figure 1: Filtering Process Example ................................................................. 69
Figure 2: Applying an IP Filter to an Ingress Interface ...................................... 76
Preface

About This Guide

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

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 OS documentation set is composed of the following books:

- **7210-SAS D, E OS Basic System Configuration Guide**
  This guide describes basic system configurations and operations.

- **7210-SAS D, E OS System Management Guide**
  This guide describes system security and access configurations as well as event logging and accounting logs.

- **7210-SAS D, E OS Interface Configuration Guide**
  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.

- **7210-SAS D, E OS Router Configuration Guide**
  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP and MAC-based filtering.

- **7210-SAS D, E 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 OS Services Guide**
  This guide describes how to configure service parameters such as customer information, and user services.

- **7210-SAS D, E OS OAM and Diagnostic Guide**
  This guide describes how to configure features such as servicemirroring and Operations, Administration and Management (OAM) tools.

- **7210-SAS D, E 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://www1.alcatel-lucent.com/comps/pages/carrier_support.jhtml
Preface
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

<table>
<thead>
<tr>
<th>Area</th>
<th>Task</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router configuration</td>
<td>Configure router parameters, including router interfaces and addresses and router IDs.</td>
<td>IP Router Configuration on page 15</td>
</tr>
<tr>
<td></td>
<td>IP and MAC filters</td>
<td>Filter Policies on page 59</td>
</tr>
<tr>
<td>Reference</td>
<td>List of IEEE, IETF, and other proprietary entities.</td>
<td>Standards and Protocol Support on page 825</td>
</tr>
</tbody>
</table>
IP Router Configuration

In This Chapter

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

Topics in this chapter include:

• Configuring IP Router Parameters on page 16
  → Interfaces on page 16
• Configuration Notes on page 18
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 with 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 on page 16

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.
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 caveats.

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

This section provides information to configure an IP router.

Topics in this section include:

- Router Configuration Overview on page 20
- Basic Configuration on page 21
- Common Configuration Tasks on page 22
  → Configuring a System Name on page 22
  → Configuring Interfaces on page 23
  → Configuring a System Interface on page 23
- Service Management Tasks on page 24
  → Changing the System Name on page 24
  → Modifying Interface Parameters on page 36
  → Deleting a Logical IP Interface on page 25
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 on page 22
- Configuring Interfaces on page 23
  → Configuring a System Interface on page 23

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])
```
Service Management Tasks

This section discusses the following service management tasks:

- Changing the System Name on page 24
- Modifying Interface Parameters on page 36
- Deleting a Logical IP Interface on page 25

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#
#------------------------------------------
# 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:**
```
cfg-router(config-router)# no interface ip-int-name
```

**Example:**
```
cfg-router(config-router)# interface test-interface
  cfg-router(config-router-if)# shutdown
  cfg-router(config-router-if)# exit
  cfg-router(config-router)# no interface test-interface
  cfg-router(config-router)#
```
IP Router Command Reference

Command Hierarchies

Configuration Commands

- Router Commands on page 28
- Router Interface Commands on page 29
- Router Advertisement Commands on page 47
- Show Commands on page 30
- Clear Commands on page 31
- Debug Commands on page 31
IP Router Command Reference

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
    [no] address {ip-address/mask | ip-address netmask} broadcast {all-ones | host-ones}
    no address
    description description-string
    no description
    [no] icmp
      redirects [number seconds]
      no redirects
      ttl-expired [number seconds]
      no ttl-expired
      unreachable [number seconds]
      [no] filter
    [no] loopback
    [no] shutdown
```
Show Commands

```
show
    -- router router-instance
        -- arp [ ip-int-name | ip-address/mask | mac ieee-mac-address | summary ] [local | dynamic | static]
        -- interface [ ip-address | ip-int-name ] [detail] [family]
        -- interface <ip-address | ip-int-name> statistics
        -- route-table <ip-address/mask> [longer|exact][summary]
        -- static-arp [ ip-address | ip-int-name | mac ieee-mac-addr]
        -- static-route [family] [ip-prefix/mask] [preference preference] [next-hop ip-address]
            [detail]
        -- status
```
Clear Commands

clear
  — router [router-instance]
  — arp {all | ip-addr | interface {ip-int-name | ip-addr}}

Debug Commands

d debug
  — trace
  — router router-instance
    — ip
      — [no] arp
      — icmp
      — no icmp
      — [no] interface [ip-int-name | ip-address]
      — 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.

Default Base

static-route

[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.

<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-prefix</td>
<td>a.b.c.d (host bits must be 0)</td>
</tr>
<tr>
<td>ipv4-prefix-length</td>
<td>0 — 32</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>x:x:x:x:x:x:x (eight 16-bit pieces)</td>
</tr>
<tr>
<td></td>
<td>x:x:x:x:d.d.d.d</td>
</tr>
<tr>
<td></td>
<td>x [0 — FFFF]H</td>
</tr>
<tr>
<td></td>
<td>d [0 — 255]D</td>
</tr>
<tr>
<td>ipv6-prefix-length</td>
<td>0 — 128</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address</td>
<td>a.b.c.d (host bits must be 0)</td>
</tr>
</tbody>
</table>

netmask — The subnet mask in dotted decimal notation.

<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0 — 255.255.255.255</td>
<td>(network bits all 1 and host bits all 0)</td>
</tr>
</tbody>
</table>
**preference** *preference* — The preference of this static route versus the routes from different sources such as OSPF, expressed as a decimal integer. When modifying the preference of an existing static route, the metric will not be changed unless specified.

Different protocols should not be configured with the same preference.

If 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.

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

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

**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.
Configuration Commands

**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.
address

**Syntax**

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

**Context**

config>router>interface

**Description**

This command assigns an IP address to 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 immediately 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 indicates 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

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.
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]

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]

Context  

Description  

Parameters  

- number — The maximum number of ICMP redirect messages to send, expressed as a decimal integer.
  
  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
**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.
Show Commands

arp

**Syntax**

```bash
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-address` — 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:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the ARP entry.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the ARP entry.</td>
</tr>
<tr>
<td>Expiry</td>
<td>The age of the ARP entry.</td>
</tr>
<tr>
<td>Type</td>
<td>Dyn — The ARP entry is a dynamic ARP entry.</td>
</tr>
<tr>
<td></td>
<td>Inv — The ARP entry is an inactive static ARP entry (invalid).</td>
</tr>
<tr>
<td></td>
<td>Oth — The ARP entry is a local or system ARP entry.</td>
</tr>
<tr>
<td></td>
<td>Sta — The ARP entry is an active static ARP entry.</td>
</tr>
<tr>
<td>Int</td>
<td>The ARP entry is an internal ARP entry.</td>
</tr>
<tr>
<td>[I]</td>
<td>The ARP entry is in use.</td>
</tr>
<tr>
<td>Interface</td>
<td>The IP interface name associated with the ARP entry.</td>
</tr>
<tr>
<td>No. of ARP Entries</td>
<td>The number of ARP entries displayed in the list.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
*B:7710-Red-RR# show router arp

===============================================================================
ARP Table (Router: Base)
===============================================================================
<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Expiry</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
</table>
```

7210 SAS D, E OS Router Configuration Guide
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.

Values 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.

interface

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

Context show>router

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

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

detail — Displays detailed IP interface information.

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

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface-Name</td>
<td>The IP interface name.</td>
</tr>
<tr>
<td>Type</td>
<td>n/a — No IP address has been assigned to the IP interface, so the IP address type is not applicable.</td>
</tr>
<tr>
<td></td>
<td>Pri — The IP address for the IP interface is the Primary address on the IP interface.</td>
</tr>
</tbody>
</table>
### Label | Description (Continued)
---|---
**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.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Name</td>
<td>The IP interface name.</td>
</tr>
<tr>
<td>Admin</td>
<td>Down — The IP interface is administratively disabled.</td>
</tr>
</tbody>
</table>
### 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:*  If Type : IES
 TOS Marking  : Untrusted  IES ID    : 100
 SNTP B.Cast  : False  Arp Timeout : 14400
 MAC Address  : 2e:59:01:00:02  Arp Timeout : 14400
 IP MTU       : 1500
 ICMPF Details
```

### Table

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

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest Address</td>
<td>The route destination address and mask.</td>
</tr>
</tbody>
</table>
A:ALA# show router route-table

Route Table (Router: Base)

<table>
<thead>
<tr>
<th>Dest Prefix</th>
<th>Type</th>
<th>Proto</th>
<th>Age</th>
<th>Metric</th>
<th>Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1/32</td>
<td>Remote</td>
<td>Static</td>
<td>00h22m29s</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6.6.6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2.2/32</td>
<td>Local</td>
<td>Local</td>
<td>00h22m52s</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>5.5.5.0/24</td>
<td>Remote</td>
<td>Static</td>
<td>00h22m29s</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6.6.6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.6.6.0/24</td>
<td>Local</td>
<td>Local</td>
<td>00h22m30s</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>to-PE-E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No. of Routes: 4

A:ALA#

B:ALA-B# show router route-table 100.10.0.0 exact

Route Table (Router: Base)

<table>
<thead>
<tr>
<th>Dest Address</th>
<th>Next Hop</th>
<th>Type</th>
<th>Proto</th>
<th>Age</th>
<th>Metric</th>
<th>Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.10.0.0/16</td>
<td></td>
<td>Black Hole</td>
<td>Remote</td>
<td>Static</td>
<td>00h03m17s</td>
<td>5</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Direct</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Total</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

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.

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

**Sample Output**

A:ALA-A# `show router static-arp`

```
ARP Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Age</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.200.0.253</td>
<td>00:00:5a:40:00:01</td>
<td>00:00:00:00</td>
<td>Sta</td>
<td>to-ser1</td>
</tr>
</tbody>
</table>
```
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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Age</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.200.1.1</td>
<td>00:00:5a:01:00:33</td>
<td>00:00:00</td>
<td>Inv</td>
<td>to-ser1</td>
</tr>
</tbody>
</table>

A:ALA-A#

A:ALA-A# show router static-arp to-ser1

ARP Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Age</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.200.0.253</td>
<td>00:00:5a:40:00:01</td>
<td>00:00:00</td>
<td>Sta</td>
<td>to-ser1</td>
</tr>
</tbody>
</table>

A:ALA-A#

A:ALA-A# show router static-arp mac 00:00:5a:40:00:01

ARP Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Age</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.200.0.253</td>
<td>00:00:5a:40:00:01</td>
<td>00:00:00</td>
<td>Sta</td>
<td>to-ser1</td>
</tr>
</tbody>
</table>

A:ALA-A#

**static-route**

**Syntax**

```
static-route [ip-prefix lmask] | [preference preference] | [next-hop ip-address]
```

**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 lmask** — Displays static routes only matching the specified ip-prefix and mask.
  - **Values**
    - ipv4-prefix: a.b.c.d (host bits must be 0)
    - ipv4-prefix-length: 0 — 32

- **preference preference** — Only displays static routes with the specified route preference.
  - **Values**
    - 0 — 65535
next-hop ip-address — Only displays static routes with the specified next hop IP address.

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

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

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addr/mask</td>
<td>The static route destination address and mask.</td>
</tr>
<tr>
<td>Pref</td>
<td>The route preference value for the static route.</td>
</tr>
<tr>
<td>Metric</td>
<td>The route metric value for the static route.</td>
</tr>
<tr>
<td>Type</td>
<td>BH — The static route is a black hole route. The Nexthop for this type of</td>
</tr>
<tr>
<td></td>
<td>route is black-hole.</td>
</tr>
<tr>
<td></td>
<td>NH — The route is a static route with a directly connected next hop. The</td>
</tr>
<tr>
<td></td>
<td>Nexthop for this type of route is either the next hop IP address or an</td>
</tr>
<tr>
<td></td>
<td>egress IP interface name.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The next hop for the static route destination.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol through which the route was learned.</td>
</tr>
<tr>
<td>Interface</td>
<td>The egress IP interface name for the static route.</td>
</tr>
<tr>
<td></td>
<td>n/a — indicates there is no current egress interface because the static</td>
</tr>
<tr>
<td></td>
<td>route is inactive or a black hole route.</td>
</tr>
<tr>
<td>Active</td>
<td>N — The static route is inactive; for example, the static route is disabled</td>
</tr>
<tr>
<td></td>
<td>or the next hop IP interface is down.</td>
</tr>
<tr>
<td></td>
<td>Y — The static route is active.</td>
</tr>
<tr>
<td>No. of Routes</td>
<td>The number of routes displayed in the list.</td>
</tr>
</tbody>
</table>

Sample Output

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

A:ALA-A# show router static-route 192.168.250.0/24
---------------------------------------------------------------------------------------------------------------------
Route Table
Show Commands

<table>
<thead>
<tr>
<th>IP Addr/mask</th>
<th>Pref Metric</th>
<th>Type</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.250.0/24</td>
<td>5</td>
<td>1</td>
<td>ID</td>
<td>10.200.10.1</td>
<td>to-ser1</td>
</tr>
</tbody>
</table>

A:ALA-A#

A:ALA-A# show router static-route preference 4

<table>
<thead>
<tr>
<th>IP Addr/mask</th>
<th>Pref Metric</th>
<th>Type</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.254.0/24</td>
<td>4</td>
<td>1</td>
<td>BH</td>
<td>black-hole</td>
<td>n/a</td>
</tr>
</tbody>
</table>

A:ALA-A#

A:ALA-A# show router static-route next-hop 10.10.0.254

<table>
<thead>
<tr>
<th>IP Addr/mask</th>
<th>Pref Metric</th>
<th>Type</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.253.0/24</td>
<td>5</td>
<td>1</td>
<td>NH</td>
<td>10.10.0.254</td>
<td>n/a</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>The administrative and operational states for the router.</td>
</tr>
<tr>
<td>Max Routes</td>
<td>The maximum number of routes configured for the system.</td>
</tr>
<tr>
<td>Total Routes</td>
<td>The total number of routes in the route table.</td>
</tr>
</tbody>
</table>

Sample Output

A:DUT-B>show>router# show router status

Router Status (Router: Base)
<table>
<thead>
<tr>
<th>Admin State</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Up</td>
</tr>
<tr>
<td>Max Routes</td>
<td>10000</td>
</tr>
<tr>
<td>Total IPv4 Routes</td>
<td>5</td>
</tr>
<tr>
<td>ECMP Max Routes</td>
<td>1</td>
</tr>
</tbody>
</table>

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.
```
Debug Commands

router

<table>
<thead>
<tr>
<th>Syntax</th>
<th>router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>debug</td>
</tr>
<tr>
<td>Description</td>
<td>This command configures debugging for a router instance.</td>
</tr>
<tr>
<td>Parameters</td>
<td>router-instance — Specify the router name or service ID.</td>
</tr>
<tr>
<td>Values</td>
<td>service-id: 1 — 2147483647</td>
</tr>
<tr>
<td>Default</td>
<td>Base</td>
</tr>
</tbody>
</table>

ip

<table>
<thead>
<tr>
<th>Syntax</th>
<th>ip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>debug&gt;router</td>
</tr>
<tr>
<td>Description</td>
<td>This command configures debugging for IP.</td>
</tr>
</tbody>
</table>

arp

<table>
<thead>
<tr>
<th>Syntax</th>
<th>arp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>debug&gt;router&gt;ip</td>
</tr>
<tr>
<td>Description</td>
<td>This command configures route table debugging.</td>
</tr>
</tbody>
</table>

icmp

<table>
<thead>
<tr>
<th>Syntax</th>
<th>[no] icmp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>debug&gt;router&gt;ip</td>
</tr>
<tr>
<td>Description</td>
<td>This command enables ICMP debugging.</td>
</tr>
</tbody>
</table>
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)
  - ipv6-address    x:x:x:x:x:x:x:x (eight 16-bit pieces)
  - x:x:x:x:x:x: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.

\- **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: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, hexadecimal, 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 pre-
fix 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 on page 60
  → Service-Based Filtering on page 60
  → Filter Policy Entities on page 61
  → Redirect Policies on page 92
  → VID Filters on page 97
- Creating and Applying Policies on page 63
- Configuration Notes on page 71
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 criteria.

Only one ingress IP or MAC filter policy and one egress IP or MAC filter policy can be applied to a Layer 2 SAP. Only one ingress IP filter policy and one egress IP filter policy can be applied to a Layer 3 SAP.

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

Table 2: Applying Filter Policies

<table>
<thead>
<tr>
<th>IP Filter</th>
<th>MAC Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRON TOD-suite</td>
<td>CRON TOD-suite</td>
</tr>
<tr>
<td>VLL SAP</td>
<td>VLL SAP</td>
</tr>
<tr>
<td>IES interface SAP</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Filter policies can be applied to specific service types:

- Epipe — Both MAC and IP filters are supported on an Epipe SAP.
- VPLS — Both MAC and IP filters are supported on a VPLS SAP.
- VPRN — Only IP filters are supported on VPRN SAP.

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.
Filter Policy Configuration Overview

- **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 interfaces** — IP filter policies are applied to IES SAPs.
Creating and Applying Policies

START

CREATE AN IP OR MAC FILTER (FILTER ID) ➔ SPECIFY SCOPE, DEFAULT ACTION, DESCRIPTION

CREATE FILTER ENTRIES (ENTRY ID) ➔ SPECIFY ACTION, PACKET MATCHING CRITERIA

CREATE SERVICE

ASSOCIATE FILTER ID

SAVE CONFIGURATION
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).

- **Destination IP address and mask** — Destination IP address and mask values can be entered as search criteria.

- **Protocol** — Entering a protocol ID (such as TCP, UDP, etc.) allows the filter to search for the protocol specified in this field.

- **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 3, DSCP Name to DSCP Value Table, on page 66.

- **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.

- **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 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 or xx-xx-xx-xx-xx-xx; for example, 02:dc:98:1d:00:01.

- **Dot1p and mask**
  Entering an IEEE 802.1p value or range allows the filter to search for matching 802.1p frame. The Dot1p and mask accepts decimal, hex, or binary in the range of 0 to 7.

- **Ethertype**
  Entering an Ethernet type II Ethertype value to be used as a filter match criterion. The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. The Ethertype accepts decimal, hex, or binary in the range of 1536 to 65535.
## DSCP Values

Table 3: DSCP Name to DSCP Value Table

<table>
<thead>
<tr>
<th>DSCP Name</th>
<th>Decimal DSCP Value</th>
<th>Hexadecimal DSCP Value</th>
<th>Binary DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp1</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp2</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp3</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp4</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp6</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp7</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cs1</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp9</td>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af10</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af11</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af12</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp13</td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp14</td>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp15</td>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cs2</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp17</td>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af21</td>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp19</td>
<td>19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af22</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp21</td>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af23</td>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp23</td>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cs3</td>
<td>24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp25</td>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af31</td>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp27</td>
<td>27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af32</td>
<td>28</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp29</td>
<td>29</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3: DSCP Name to DSCP Value Table  (Continued)

<table>
<thead>
<tr>
<th>DSCP Name</th>
<th>Decimal DSCP Value</th>
<th>Hexadecimal DSCP Value</th>
<th>Binary DSCP Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>af33</td>
<td>30</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp21</td>
<td>31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cs4</td>
<td>32</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp33</td>
<td>33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af41</td>
<td>34</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp35</td>
<td>35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af42</td>
<td>36</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp37</td>
<td>37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>af43</td>
<td>38</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp39</td>
<td>39</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cs5</td>
<td>40</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp41</td>
<td>41</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp42</td>
<td>42</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp43</td>
<td>43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp44</td>
<td>44</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp45</td>
<td>45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ef</td>
<td>46</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp47</td>
<td>47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nc1</td>
<td>48</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp49</td>
<td>49</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp50</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp51</td>
<td>51</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp52</td>
<td>52</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp53</td>
<td>53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp54</td>
<td>54</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp55</td>
<td>55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp56</td>
<td>56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp57</td>
<td>57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nc2</td>
<td>58</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>cp60</td>
<td>60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp61</td>
<td>61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>cp62</td>
<td>62</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 1 displays an example of several packets forwarded upon matching the filter criteria and several packets traversing through the filter entries and then dropped.

**Figure 1: Filtering Process Example**

-ingress packets:

1. Source Address: 10.10.10.103, Destination Address: 10.10.10.104
2. Source Address: 10.10.10.103, Destination Address: 10.10.10.105
3. Source Address: 10.10.10.103, Destination Address: 10.10.10.106

Filter ID: 5
-Default Action: Drop
-Filter Entries: 10 (Action: Forward), 20 (Action: Forward), 30 (Action: Forward)

Search Criteria:
-Source Address: 10.10.10.103
-Destination Address: 10.10.10.104

Filter Entry ID: 10
-Source Address: 10.10.10.103
-Destination Address: 10.10.10.104
-Action: Forward

N

Filter Entry ID: 20
-Source Address: 10.10.10.103
-Destination Address: 10.10.10.105
-Action: Forward

N

Filter Entry ID: 30
-Source Address: 10.10.10.103
-Destination Address: 10.10.10.106
-Action: Forward

Y

Remaining packets are dropped per the default action (Drop)

SA: 10.10.10.103, DA: 10.10.10.107
SA: 10.10.10.103, DA: 10.10.10.108
SA: 10.10.10.192, DA: 10.10.10.16
SA: 10.10.10.155, DA: 10.10.10.21
Applying Filters

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

- Applying a Filter to a SAP on page 70
- Applying a Filter to an IES Interface on page 70

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

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.
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.
- MAC filters cannot be applied to network interfaces.
- 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 M, the default frame-format is “EthernetII”

<table>
<thead>
<tr>
<th>Frame Format</th>
<th>Etype</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet – II</td>
<td>Yes</td>
</tr>
<tr>
<td>802.3</td>
<td>No</td>
</tr>
<tr>
<td>802.3 – snap</td>
<td>No</td>
</tr>
<tr>
<td>802.3-llc</td>
<td>No</td>
</tr>
</tbody>
</table>
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.
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 on page 76
- Common Configuration Tasks on page 77
  - Creating an IP Filter Policy on page 77
  - Applying Filter Policies on page 83
- Filter Management Tasks on page 85
  - Renumbering Filter Policy Entries on page 85
  - Modifying an IP Filter Policy on page 87
  - Deleting a Filter Policy on page 90
  - Deleting a Filter Policy on page 90
  - Copying Filter Policies on page 92
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

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. Figure 2 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#
```

**Figure 2: 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 77
- Creating a MAC Filter Policy on page 80
- Applying Filter Policies on page 83

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

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"
macth
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 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#
```
The following displays a filter matching configuration example.

```
A:ALA-7>config>filter>mac-filter# info
----------------------------------------------
description "filter-west"
scope exclusive
table 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
----------------------------------------------
A:ALA-7>config>filter#
```
Applying Filter Policies

Filter policies can be associated with the following entities:

Table 5: Applying Filter Policies

<table>
<thead>
<tr>
<th>IP Filter</th>
<th>MAC Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epipe SAP</td>
<td>Epipe SAP</td>
</tr>
<tr>
<td>IES interface SAP</td>
<td>N/A</td>
</tr>
<tr>
<td>VPLS SAP</td>
<td>VPLS SAP</td>
</tr>
</tbody>
</table>

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 create
      ingress
      filter ip 10
      exit
gress
      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 on page 85
- Modifying an IP Filter Policy on page 87
- Deleting a Filter Policy on page 90
- Copying Filter Policies on page 92

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

...
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:

```plaintext
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:

```plaintext
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 10.10.10.432
         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
      dst-mac 02:dc:98:1d:00:01 ff:ff:ff:ff:ff
    exit
    action forward
  exit
entry 2 create
  match
    dot1p 7 7
  exit
  action drop
  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 90
- From an Egress SAP on page 90
- From the Filter Configuration on page 91

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

- IP Filter Policy Commands on page 93
- MAC Filter Policy Commands on page 94
- Redirect Policy Configuration Commands on page 123
- Generic Filter Commands on page 95
- Show Commands on page 95
- Clear Commands on page 95
- Monitor Commands on page 95

Configuration Commands

IP Filter Policy Commands

```bash
config
  filter
    ip-filter filter-id [create]
    no ip-filter filter-id
      default-action {drop | forward}
      description description-string
      no description
      renum old-entry-id new-entry-id
      scope {exclusive | template}
      no scope
      entry entry-id [time-range time-range-name] [create]
      no entry entry-id
        action [drop]
        action forward
        no action
        description description-string
        no description
        match [protocol protocol-id]
        no match
          dscp dscp-name
          no dscp
          dst-ip {ip-address/mask | ip-address netmask}
          no dst-ip
          dst-port {eq} dst-port-number
          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}
```

Filter Policies
Filter Command Reference

MAC Filter Policy Commands

config
  filter
    mac-filter filter-id [create]
    no mac-filter filter-id
      default-action {drop | forward}
      description description-string
      no description
    entry entry-id [time-range time-range-name]
    no entry entry-id [create]
      description description-string
      no description
      action [drop]
      action forward
      no action
      match
      no match
        dot1p dot1p-value [dot1p-mask]
        no dot1p
        dst-mac ieee-address [ieee-address-mask]
        no dst-mac
        etype 0x0600..0xffff
        no etype
        src-mac ieee-address [ieee-address-mask]
        no src-mac
    renum old-entry-id new-entry-id
    scope {exclusive | template}
    no scope
Generic Filter Commands

```
config
  filter
    copy ip-filter | mac-filter src-filter-id [src-entry src-entry-id] to dst-filter-id [dst-entry dst-entry-id] [overwrite]
```

Show Commands

```
show
  filter
    download-failed
    ip [ip-filter-id [entry entry-id] [association | counters]
    mac {mac-filter-id [entry entry-id] [association | counters]}
```

Clear Commands

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

Monitor Commands

```
monitor
  filter
    ip ip-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**

<table>
<thead>
<tr>
<th>description string</th>
</tr>
</thead>
<tbody>
<tr>
<td>no description</td>
</tr>
</tbody>
</table>

**Context**

- config>filter>ip-filter
- config>filter>ip-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 [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.

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.

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>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>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>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 immediately 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
```

**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
```

**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, hexadecimal, or binary - DHB)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Protocol ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp</td>
<td>1</td>
<td>Internet Control Message</td>
</tr>
<tr>
<td>igmp</td>
<td>2</td>
<td>Internet Group Management</td>
</tr>
<tr>
<td>ip</td>
<td>4</td>
<td>IP in IP (encapsulation)</td>
</tr>
<tr>
<td>tcp</td>
<td>6</td>
<td>Transmission Control</td>
</tr>
<tr>
<td>egp</td>
<td>8</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>igp</td>
<td>9</td>
<td>Any private interior gateway (used by Cisco for IGRP)</td>
</tr>
<tr>
<td>udp</td>
<td>17</td>
<td>User Datagram</td>
</tr>
<tr>
<td>rdp</td>
<td>27</td>
<td>Reliable Data Protocol</td>
</tr>
<tr>
<td>idrp</td>
<td>45</td>
<td>Inter-Domain Routing Protocol</td>
</tr>
<tr>
<td>rsvp</td>
<td>46</td>
<td>Reservation Protocol</td>
</tr>
<tr>
<td>gre</td>
<td>47</td>
<td>General Routing Encapsulation</td>
</tr>
<tr>
<td>iso-ip</td>
<td>80</td>
<td>ISO Internet Protocol</td>
</tr>
<tr>
<td>eigrp</td>
<td>88</td>
<td>EIGRP</td>
</tr>
<tr>
<td>ospf-igp</td>
<td>89</td>
<td>OSPFIGP</td>
</tr>
<tr>
<td>ether-ip</td>
<td>97</td>
<td>Ethernet-within-IP Encapsulation</td>
</tr>
<tr>
<td>encaps</td>
<td>98</td>
<td>Encapsulation Header</td>
</tr>
<tr>
<td>pnni</td>
<td>102</td>
<td>PNNI over IP</td>
</tr>
<tr>
<td>pim</td>
<td>103</td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td>vrrp</td>
<td>112</td>
<td>Virtual Router Redundancy Protocol</td>
</tr>
<tr>
<td>l2tp</td>
<td>115</td>
<td>Layer Two Tunneling Protocol</td>
</tr>
<tr>
<td>stp</td>
<td>118</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>ptp</td>
<td>123</td>
<td>Performance Transparency Protocol</td>
</tr>
<tr>
<td>isis</td>
<td>124</td>
<td>ISIS over IPv4</td>
</tr>
<tr>
<td>crtp</td>
<td>126</td>
<td>Combat Radio Transport Protocol</td>
</tr>
<tr>
<td>crudp</td>
<td>127</td>
<td>Combat Radio User Datagram</td>
</tr>
</tbody>
</table>
MAC Filter Entry Commands

**action**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>action drop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>action forward</td>
</tr>
<tr>
<td></td>
<td>no action</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>match</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no match</td>
</tr>
</tbody>
</table>

**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
```

**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[netmask]} [netmask]
no dst-ip
```

**Context**

```
config>filter>ip-filter>entry>match
```

**Description**

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

To match on the destination IP address, specify the address and its associated mask, 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-prefix` — 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 expressed in dotted quad notation.

  **Values**
  
  0.0.0.0 — 255.255.255.255
**dst-port**

**Syntax**

`dst-port {eq} dst-port-number`

`no dst-port`

**Context**

`config>filter>ip-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`

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-code</td>
<td>The ICMP code values that must be present to match.</td>
</tr>
<tr>
<td>Values</td>
<td>0 — 255</td>
</tr>
</tbody>
</table>

icmp-type

Syntax

```
icmp-type icmp-type
no icmp-type
```

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

Description

This command configures matching on the ICMP type field in the ICMP header of an IP 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-type</td>
<td>The ICMP type values that must be present to match.</td>
</tr>
<tr>
<td>Values</td>
<td>0 — 255</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>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.</td>
</tr>
<tr>
<td>false</td>
<td>Specifies matching on IP packets that do not have any option field present in the IP header.</td>
</tr>
</tbody>
</table>
**src-ip**

**Syntax**  
```
src-ip {ip-address[mask]} [netmask]
no src-ip
```

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

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

To match on the source IP address, specify the address and its associated mask, e.g. 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.

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

**Default**  
```
o 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 expressed 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
```

**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**  
```
o 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

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

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:

<table>
<thead>
<tr>
<th>Format Style</th>
<th>Format Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>D</td>
<td>4</td>
</tr>
<tr>
<td>Hexadecimal</td>
<td>0xH</td>
<td>0x4</td>
</tr>
<tr>
<td>Binary</td>
<td>0bBBB</td>
<td>0b100</td>
</tr>
</tbody>
</table>

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  
\texttt{dst-mac \textit{ieee-address} [mask]}
\texttt{no dst-mac}

Context  \texttt{config>filter>mac-filter>entry>match}

Description  
Configures a destination MAC address or range to be used as a MAC filter match criterion. The \texttt{no} form of the command removes the destination mac address as the match criterion.

Default  
\texttt{no dst-mac}

Parameters  
\textit{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

\textit{mask} — A 48-bit mask to match a range of MAC address values.

This 48-bit mask can be configured using the following formats:

<table>
<thead>
<tr>
<th>Format Style</th>
<th>Format Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>DDDDDDDDDDDDDDD</td>
<td>281474959933440</td>
</tr>
<tr>
<td>Hexadecimal</td>
<td>0xHHHHHHHHHHHH</td>
<td>0xFFFF000000</td>
</tr>
<tr>
<td>Binary</td>
<td>0bBBBBBBBB...B</td>
<td>0b11110000...B</td>
</tr>
</tbody>
</table>

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 0xFFFF000000

Default  
\texttt{0xFFFF000000 (exact match)}

Values  
0x00000000000000 — 0xFFFF000000

etype

Syntax  
\texttt{etype \textit{ethernet-type}}
\texttt{no etype}

Context  \texttt{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 \texttt{no} form of the command removes the previously entered etype field as the match criteria.

Default  
\texttt{no etype}
**Parameters**

*ethernet-type* — The Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.

**Values**

0x0600 — 0xFFFF

**src-mac**

**Syntax**

def src-mac ieee-address [ieee-address-mask]
def 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:

<table>
<thead>
<tr>
<th>Format Style</th>
<th>Format Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>DDDDDDDDDDDDDD</td>
<td>28147495933440</td>
</tr>
<tr>
<td>Hexadecimal</td>
<td>0xHHHHHHHHHHHH</td>
<td>0xFFFFF000000</td>
</tr>
<tr>
<td>Binary</td>
<td>0bBBBBBBBB...B</td>
<td>0b11110000...B</td>
</tr>
</tbody>
</table>

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 0xFFFFF000000

**Default**

0xFFFFF000000 (exact match)

**Values**

0x00000000000000 — 0xFFFFF000000
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. 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.

**Parameters**
- **ip-filter** — Indicates that the source-filter-id and the dest-filter-id are IP filter IDs.
- **mac-filter** — Indicates that the source-filter-id and the dest-filter-id are MAC filter IDs.
- **source-filter-id** — The source-filter-id identifies the source filter policy from which the copy command will attempt to copy. The filter policy must exist within the context of the preceding keyword (ip-filter or mac-filter).
- **dest-filter-id** — The dest-filter-id identifies the destination filter policy to which the copy command will attempt to copy. If the overwrite keyword does not follow, the filter policy ID cannot already exist within the system for the filter type the copy command is issued for. If the overwrite keyword is present, the destination policy ID may or may not exist.
- **overwrite** — The overwrite keyword specifies that the destination filter ID may exist. If it does, everything in the existing destination filter ID will be completely overwritten with the contents of the source filter ID. If the destination filter ID exists, either overwrite must be specified or an error message will be returned. If overwrite is specified, the function of copying from source to destination occurs in a ‘break before make’ manner and therefore should be handled with care.

**renum**

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

**Context**
```
config>filter>ip-filter
config>filter>mac-filter
```

**Description**
This command renumbers existing MAC or IP filter entries to properly sequence filter entries. This may be required in some cases since the OS exits when the first match is found and executes the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

**Parameters**
- **old-entry-id** — Enter the entry number of an existing entry.
  - **Values**
    - 1 — 65535
new-entry-id — Enter the new entry-number to be assigned to the old entry.

Values 1 — 65535
Show Commands

download-failed

Syntax

```
download-failed
```

Context

```
show>filter
```

Description

This command shows all filter entries for which the download has failed.

Output

download-failed Output — The following table describes the filter download-failed output.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter-type</td>
<td>Displays the filter type.</td>
</tr>
<tr>
<td>Filter-ID</td>
<td>Displays the ID of the filter.</td>
</tr>
<tr>
<td>Filter-Entry</td>
<td>Displays the entry number of the filter.</td>
</tr>
</tbody>
</table>

Sample Output

```
A:ALA-48# show filter download-failed

Filter entries for which download failed

<table>
<thead>
<tr>
<th>Filter-type</th>
<th>Filter-ID</th>
<th>Filter-Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>1</td>
<td>10</td>
</tr>
</tbody>
</table>

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
Show Commands

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.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Id</td>
<td>The IP filter ID</td>
</tr>
<tr>
<td>Scope</td>
<td>Template — The filter policy is of type template.</td>
</tr>
<tr>
<td></td>
<td>Exclusive — The filter policy is of type exclusive.</td>
</tr>
<tr>
<td>Applied</td>
<td>No — The filter policy ID has not been applied.</td>
</tr>
<tr>
<td></td>
<td>Yes — The filter policy ID is applied.</td>
</tr>
<tr>
<td>Description</td>
<td>The IP filter policy description.</td>
</tr>
</tbody>
</table>

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
===============================================================================

Output

Show Filter (with filter-id specified) — The following table describes the command output for the command when a filter ID is specified.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Id</td>
<td>The IP filter policy ID.</td>
</tr>
<tr>
<td>Scope</td>
<td>Template – The filter policy is of type template.</td>
</tr>
<tr>
<td></td>
<td>Exclusive – The filter policy is of type exclusive.</td>
</tr>
<tr>
<td>Entries</td>
<td>The number of entries configured in this filter ID.</td>
</tr>
<tr>
<td>Description</td>
<td>The IP filter policy description.</td>
</tr>
<tr>
<td>Applied</td>
<td>No – The filter policy ID has not been applied.</td>
</tr>
<tr>
<td></td>
<td>Yes – The filter policy ID is applied.</td>
</tr>
<tr>
<td>Def. Action</td>
<td>Forward – The default action for the filter ID for packets that do not match the filter entries is to forward.</td>
</tr>
<tr>
<td></td>
<td>Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.</td>
</tr>
<tr>
<td>Filter Match Criteria</td>
<td>IP – Indicates the filter is an IP filter policy.</td>
</tr>
<tr>
<td>Entry</td>
<td>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.</td>
</tr>
<tr>
<td>ICMP Type</td>
<td>The ICMP type match criterion. Undefined indicates no ICMP type specified.</td>
</tr>
<tr>
<td>Fragment</td>
<td>False – Configures a match on all non-fragmented IP packets.</td>
</tr>
<tr>
<td></td>
<td>True – Configures a match on all fragmented IP packets.</td>
</tr>
<tr>
<td></td>
<td>Off – Fragments are not a matching criteria. All fragments and non-fragments implicitly match.</td>
</tr>
<tr>
<td>TCP-syn</td>
<td>False – Configures a match on packets with the SYN flag set to false.</td>
</tr>
<tr>
<td></td>
<td>True – Configured a match on packets with the SYN flag set to true.</td>
</tr>
<tr>
<td></td>
<td>Off – The state of the TCP SYN flag is not considered as part of the match criteria.</td>
</tr>
<tr>
<td>Match action</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Drop – Drop packets matching the filter entry.</td>
</tr>
</tbody>
</table>
Show Commands

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
-------------------------------------------------------------------------------
A:ALA-49>config>filter#

*A:Dut>Cconfig>filter# show filter ip fSpec-1 associations

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ing. Matches</td>
<td>The number of ingress filter matches/hits for the filter entry.</td>
</tr>
<tr>
<td>Src. Port</td>
<td>The source TCP or UDP port number.</td>
</tr>
<tr>
<td>Dest. Port</td>
<td>The destination TCP or UDP port number.</td>
</tr>
<tr>
<td>Dscp</td>
<td>The DiffServ Code Point (DSCP) name.</td>
</tr>
<tr>
<td>ICMP Code</td>
<td>The ICMP code field in the ICMP header of an IP packet.</td>
</tr>
<tr>
<td>Option-present</td>
<td>Off – Specifies not to search for packets that contain the option field or have an option field of zero.</td>
</tr>
<tr>
<td></td>
<td>On – Matches packets that contain the option field or have an option field of zero be used as IP filter match criteria.</td>
</tr>
<tr>
<td>TCP-ack</td>
<td>False – Configures a match on packets with the ACK flag set to false.</td>
</tr>
<tr>
<td></td>
<td>True – Configures a match on packets with the ACK flag set to true.</td>
</tr>
<tr>
<td></td>
<td>Off – The state of the TCP ACK flag is not considered as part of the match criteria.</td>
</tr>
<tr>
<td>Egr. Matches</td>
<td>The number of egress filter matches/hits for the filter entry.</td>
</tr>
</tbody>
</table>
Filter Policies

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# 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
Show Commands

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 Dest. Port : None
Dest. IP : 0.0.0.0/0 Protocol : 17
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

*ALA-49# show filter ip 10

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

<table>
<thead>
<tr>
<th>Filter Id</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Template</td>
</tr>
<tr>
<td>Entires</td>
<td>2</td>
</tr>
</tbody>
</table>

**Filter Match Criteria : IP**

<table>
<thead>
<tr>
<th>Entry</th>
<th>1010</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>time-range</strong></td>
<td>day</td>
</tr>
<tr>
<td>Src. IP</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Dest. IP</td>
<td>10.10.100.1/24</td>
</tr>
<tr>
<td>Protocol</td>
<td>Undefined</td>
</tr>
<tr>
<td>ICMP Type</td>
<td>Undefined</td>
</tr>
<tr>
<td>Fragment</td>
<td>Off</td>
</tr>
<tr>
<td>TCP-syn</td>
<td>Off</td>
</tr>
<tr>
<td>Match action</td>
<td>Forward</td>
</tr>
<tr>
<td>Ing. Matches</td>
<td>0</td>
</tr>
<tr>
<td>Egr. Matches</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry</th>
<th>1020</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>time-range</strong></td>
<td>night</td>
</tr>
<tr>
<td>Src. IP</td>
<td>0.0.0.0/0</td>
</tr>
<tr>
<td>Dest. IP</td>
<td>10.10.11.16</td>
</tr>
<tr>
<td>Protocol</td>
<td>Undefined</td>
</tr>
<tr>
<td>ICMP Type</td>
<td>Undefined</td>
</tr>
<tr>
<td>Fragment</td>
<td>Off</td>
</tr>
<tr>
<td>TCP-syn</td>
<td>Off</td>
</tr>
<tr>
<td>Match action</td>
<td>Forward</td>
</tr>
<tr>
<td>Ing. Matches</td>
<td>0</td>
</tr>
<tr>
<td>Egr. Matches</td>
<td>0</td>
</tr>
</tbody>
</table>

A:ALA-49#
### Output

**Show Filter Associations** — The following table describes the fields that display when the `associations` keyword is specified.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Id</td>
<td>The IP filter policy ID.</td>
</tr>
<tr>
<td>Scope</td>
<td>Template — The filter policy is of type Template.</td>
</tr>
<tr>
<td></td>
<td>Exclusive — The filter policy is of type Exclusive.</td>
</tr>
<tr>
<td>Entries</td>
<td>The number of entries configured in this filter ID.</td>
</tr>
<tr>
<td>Applied</td>
<td>No — The filter policy ID has not been applied.</td>
</tr>
<tr>
<td></td>
<td>Yes — The filter policy ID is applied.</td>
</tr>
<tr>
<td>Def. Action</td>
<td>Forward — The default action for the filter ID for packets that do not</td>
</tr>
<tr>
<td></td>
<td>match the filter entries is to forward.</td>
</tr>
<tr>
<td></td>
<td>Drop — The default action for the filter ID for packets that do not</td>
</tr>
<tr>
<td></td>
<td>match the filter entries is to drop.</td>
</tr>
<tr>
<td>Service Id</td>
<td>The service ID on which the filter policy ID is applied.</td>
</tr>
<tr>
<td>SAP</td>
<td>The Service Access Point on which the filter policy ID is applied.</td>
</tr>
<tr>
<td>(Ingress)</td>
<td>The filter policy ID is applied as an ingress filter policy on the interface.</td>
</tr>
<tr>
<td>(Egress)</td>
<td>The filter policy ID is applied as an egress filter policy on the interface.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of service of the service ID.</td>
</tr>
</tbody>
</table>

### 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        : 1/1:1001   (Ingress)
Service Id   : 2000                             Type           :
- SAP        : 1/1:2000   (Ingress)
===============================================================================
A:ALA-49#
```
Show Commands

**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
===============================================================================
<table>
<thead>
<tr>
<th>IP Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Id</td>
</tr>
<tr>
<td>Scope</td>
</tr>
<tr>
<td>Entries</td>
</tr>
<tr>
<td>Filter Association</td>
</tr>
<tr>
<td>Tod-suite &quot;english_suite&quot;</td>
</tr>
</tbody>
</table>
===============================================================================
A:ALA-49#
```

**Output**

**Show Filter Counters** — The following table describes the output fields when the `counters` keyword is specified.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Filter</td>
<td>The IP filter policy ID.</td>
</tr>
<tr>
<td>Filter Id</td>
<td></td>
</tr>
<tr>
<td>Scope</td>
<td>Template — The filter policy is of type Template.</td>
</tr>
<tr>
<td></td>
<td>Exclusive — The filter policy is of type Exclusive.</td>
</tr>
<tr>
<td>Applied</td>
<td>No — The filter policy ID has not been applied.</td>
</tr>
<tr>
<td></td>
<td>Yes — The filter policy ID is applied.</td>
</tr>
<tr>
<td>Def. Action</td>
<td>Forward — The default action for the filter ID for packets that do not match the filter entries is to forward.</td>
</tr>
<tr>
<td></td>
<td>Drop — The default action for the filter ID for packets that do not match the filter entries is to drop.</td>
</tr>
<tr>
<td>Filter Match Criteria</td>
<td>IP — Indicates the filter is an IP filter policy.</td>
</tr>
<tr>
<td>Entry</td>
<td>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.</td>
</tr>
<tr>
<td>Ing. Matches</td>
<td>The number of ingress filter matches/hits for the filter entry.</td>
</tr>
<tr>
<td>Egr. Matches</td>
<td>The number of egress filter matches/hits for the filter entry.</td>
</tr>
</tbody>
</table>

Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.
**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 ID and its entries is produced. The following table describes the command output for the command.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Id</td>
<td>The IP filter ID</td>
</tr>
<tr>
<td>Scope</td>
<td>Template — The filter policy is of type Template.</td>
</tr>
<tr>
<td></td>
<td>Exclusiv — The filter policy is of type Exclusive.</td>
</tr>
<tr>
<td>Applied</td>
<td>No — The filter policy ID has not been applied.</td>
</tr>
<tr>
<td></td>
<td>Yes — The filter policy ID is applied.</td>
</tr>
<tr>
<td>Description</td>
<td>The MAC filter policy description.</td>
</tr>
</tbody>
</table>

and its entries is produced. The following table describes the command output for the command.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Filter Id</td>
<td>The MAC filter policy ID.</td>
</tr>
<tr>
<td>Filter Id</td>
<td>The MAC filter policy ID.</td>
</tr>
<tr>
<td>Scope</td>
<td>Template — The filter policy is of type Template.</td>
</tr>
<tr>
<td></td>
<td>Exclusiv — The filter policy is of type Exclusive.</td>
</tr>
<tr>
<td>Description</td>
<td>The IP filter policy description.</td>
</tr>
<tr>
<td>Applied</td>
<td>No — The filter policy ID has not been applied.</td>
</tr>
<tr>
<td></td>
<td>Yes — The filter policy ID is applied.</td>
</tr>
</tbody>
</table>
Sample Detailed Output

Mac Filter : 200

Filter Id : 200  
Scope : Exclusive  
Description : Forward SERVER sourced packets

Filter Match Criteria : Mac

Entry : 200  
FrameType : 802.2SNAP  

Label | Description (Continued)
--- | ---
Def. Action | Forward — The default action for the filter ID for packets that do not match the filter entries is to forward.
Drop — The default action for the filter ID for packets that do not match the filter entries is to drop.

Filter Match Criteria | MAC — Indicates the filter is an MAC filter policy.
Entry | The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
Description | The filter entry description.
FrameType | Ethernet — The entry ID match frame type is Ethernet IEEE 802.3.
Ethernet II — The entry ID match frame type is Ethernet Type II.
Src MAC | The source MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion specified for the filter entry.

Dest MAC | The destination MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion specified for the filter entry.
Dot1p | The IEEE 802.1p value for the match criteria. Undefined indicates no value is specified.

Ethertype | The Ethertype value match criterion.
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.
Filter Policies

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
Dotlp : 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
Dotlp : 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 association information is appended to the filter information. The following table describes the fields in the appended associations output.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Association</td>
<td>The filter associations displayed are for a MAC filter policy ID.</td>
</tr>
<tr>
<td>Service Id</td>
<td>The service ID on which the filter policy ID is applied.</td>
</tr>
<tr>
<td>SAP</td>
<td>The Service Access Point on which the filter policy ID is applied.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of service of the Service ID.</td>
</tr>
<tr>
<td>(Ingress)</td>
<td>The filter policy ID is applied as an ingress filter policy on the interface.</td>
</tr>
<tr>
<td>(Egress)</td>
<td>The filter policy ID is applied as an egress filter policy on the interface.</td>
</tr>
</tbody>
</table>

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.

Sample Output

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Filter</td>
<td>The MAC filter policy ID.</td>
</tr>
<tr>
<td>Filter Id</td>
<td></td>
</tr>
<tr>
<td>Scope</td>
<td>Template — The filter policy is of type Template.</td>
</tr>
<tr>
<td></td>
<td>Exclusive — The filter policy is of type Exclusive.</td>
</tr>
<tr>
<td>Description</td>
<td>The MAC filter policy description.</td>
</tr>
<tr>
<td>Applied</td>
<td>No — The filter policy ID has not been applied.</td>
</tr>
<tr>
<td></td>
<td>Yes — The filter policy ID is applied.</td>
</tr>
<tr>
<td>Def. Action</td>
<td>Forward — The default action for the filter ID for packets that do not match the filter entries is to forward.</td>
</tr>
<tr>
<td></td>
<td>Drop — The default action for the filter ID for packets that do not match the filter entries is to drop.</td>
</tr>
<tr>
<td>Filter Match Criteria</td>
<td>Mac — Indicates the filter is an MAC filter policy.</td>
</tr>
<tr>
<td>Entry</td>
<td>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.</td>
</tr>
<tr>
<td>Ing. Matches</td>
<td>The number of ingress filter matches/hits for the filter entry.</td>
</tr>
<tr>
<td>Egr. Matches</td>
<td>The number of egress filter matches/hits for the filter entry.</td>
</tr>
</tbody>
</table>

A:ALA-49# show filter mac 8 counters

Mac Filter

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Id</td>
<td>8</td>
</tr>
<tr>
<td>Scope</td>
<td>Template</td>
</tr>
<tr>
<td>Entries</td>
<td>2</td>
</tr>
<tr>
<td>Description</td>
<td>Description for Mac Filter Policy id # 8</td>
</tr>
</tbody>
</table>

Filter Match Criteria : Mac

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
<td>8</td>
</tr>
<tr>
<td>Ing. Matches : 80 pkts</td>
<td></td>
</tr>
<tr>
<td>Egr. Matches : 62 pkts</td>
<td></td>
</tr>
</tbody>
</table>

Entry : 10

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
<td>10</td>
</tr>
<tr>
<td>Ing. Matches : 80 pkts</td>
<td></td>
</tr>
<tr>
<td>Egr. Matches : 80 pkts</td>
<td></td>
</tr>
</tbody>
</table>
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.

log

Syntax  log log-id
Context  clear
Description  Clears the contents of a memory or file based filter log.
This command has no effect on a syslog based filter log.
Parameters  log-id — The filter log ID destination expressed as a decimal integer.
  Values  101 — 199

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

**ip**

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** — 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:

• SAP syntax on page 134
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:

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Encap-Type</th>
<th>Allowed Values</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>Null</td>
<td>0</td>
<td>The SAP is identified by the port.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Dot1q</td>
<td>0 — 4094</td>
<td>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.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>QinQ</td>
<td>qtag1: 0 — 4094 qtag2: 0 — 4094</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 802.3ah Ethernet OAM
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

DIFFERENTIATED SERVICES
RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev:3260)
RFC 2598 An Experied 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 for 7210 SAS-E]
RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

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

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 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

RADIUS
RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH
draft-ietf-secsch-architecture.txt SSH Protocol Architecture
draft-ietf-secsch-userauth.txt SSH Authentication Protocol
draft-ietf-secsch-transport.txt SSH Transport Layer Protocol
draft-ietf-secsch-connection.txt SSH Connection Protocol
draft-ietf-secsch-newmodes.txt SSH Transport Layer Encryption Modes

tacacs+
draft-grant-tacacs-02.txt

TCP/IP
RFC 768 UDP
<table>
<thead>
<tr>
<th>Standards and Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1350 The TFTP Protocol</td>
</tr>
<tr>
<td>RFC 791 IP</td>
</tr>
<tr>
<td>RFC 792 ICMP</td>
</tr>
<tr>
<td>RFC 793 TCP</td>
</tr>
<tr>
<td>RFC 826 ARP</td>
</tr>
<tr>
<td>RFC 854 Telnet</td>
</tr>
<tr>
<td>RFC 1519 CIDR</td>
</tr>
<tr>
<td>RFC 1812 Requirements for IPv4 Routers</td>
</tr>
<tr>
<td>RFC 2347 TFTP option Extension</td>
</tr>
<tr>
<td>RFC 2328 TFTP Blocksize Option</td>
</tr>
<tr>
<td>RFC 2349 TFTP Timeout Interval and Transfer Size option</td>
</tr>
<tr>
<td>Timing (Only on 7210 SAS-D ETR)</td>
</tr>
<tr>
<td>ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008</td>
</tr>
<tr>
<td>ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.</td>
</tr>
<tr>
<td>ITU-T G.8261 Telecommunication Standardization Section of ITU, Timing and synchronization aspects in packet networks, issued 04/2008.</td>
</tr>
<tr>
<td>ITU-T G.8262 Telecommunication Standardization Section of ITU, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007.</td>
</tr>
<tr>
<td>ITU-T G.8264 Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008.</td>
</tr>
<tr>
<td>Proprietary MIBs</td>
</tr>
<tr>
<td>ALCATEL-IGMP-SNOOPING-MIB.mib</td>
</tr>
<tr>
<td>TIMETRA-CAPABILITY-7210-SAS-E-V1v0.mib (Only for 7210 SAS-E)</td>
</tr>
<tr>
<td>TIMETRA-CAPABILITY-7210-SAS-D-V1v0.mib (Only for 7210 SAS-D)</td>
</tr>
<tr>
<td>TIMETRA-CHASSIS-MIB.mib</td>
</tr>
<tr>
<td>TIMETRA-CLEAR-MIB.mib</td>
</tr>
<tr>
<td>TIMETRA-DOT3-OAM-MIB.mib</td>
</tr>
<tr>
<td>TIMETRA-FILTER-MIB.mib</td>
</tr>
<tr>
<td>TIMETRA-GLOBAL-MIB.mib</td>
</tr>
</tbody>
</table>
INDEX

F
Filters
overview 60
applying filter
to network ports 70
to SAP 70
entities 61
entries 61
filter entry ordering 68
filter types
IP 60, 64
MAC 60, 65, 72
matching criteria
DSCP values 66
IP 64
MAC 65
packets 64
policies 61
policy entries 61
port-based filtering 60
scope 71
services 61
configuring
basic 76
IP filter policy 77
MAC filter policy 80
management tasks 85

I
IP Router
overview 16
interfaces 16
system 16
configuring
basic 21
command reference 27
interfaces 23
overview 20
service management tasks 24
system interface 20
system name 22