Configuration Commands

Generic Commands

description

Syntax **description** *string*
no description

Context config>filter>dhcp-filter
config>filter>ip-filter
config>filter>ip-filter>entry
config>filter>ipv6-filter
config>filter>log
config>filter>mac-filter
config>filter>mac-filter>entry
config>filter>redirect-policy
config>filter>redirect-policy>destination
config>filter>match-list>ip-prefix-list
config>filter>match-list>ip-filter
config>filter>match-list>port-list

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

dhcp-filter

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

Context config>filter

Description This command configures the identification number of a DHCP filter.

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

ip-filter

Syntax **ip-filter** *filter-id* [**create**]
ip-filter {*filter-id* | *filter-name*}
no ip-filter *filter-id*

Context config>filter

Description This command creates a configuration context for an IP (v4) filter policy.

The IP filter policy, sometimes referred to as an access control list (ACL), is a template that can be applied to multiple services or multiple network ports as long as the scope of the policy is template.

Any changes made to the existing policy, using any of the sub-commands, will be applied immediately to all services where this policy is applied. For this reason, when many changes are required on an ip-filter policy, it is recommended that the policy be copied to a work area. That work-in-progress policy can be modified until complete and then written over the original filter policy. Use the **config filter copy** command to maintain policies in this manner.

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

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

Values 1 — 65535

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

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

ipv6-filter

Syntax **ipv6-filter** *filter-id* [**create**]
ip-filter {*filter-id* | *filter-name*}
no ipv6-filter *ipv6-filter-id*

Context config>filter

Description This command creates a configuration context for an IP (v6) filter policy.

The IP filter policy, sometimes referred to as an access control list (ACL), is a template that can be applied to multiple services or multiple network ports as long as the scope of the policy is template.

Any changes made to the existing policy, using any of the sub-commands, will be applied immediately to all services where this policy is applied. For this reason, when many changes are required on an ip-filter policy, it is recommended that the policy be copied to a work area. That work-in-progress policy can be modified until complete and then written over the original filter policy. Use the **config filter copy** command to maintain policies in this manner.

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

Parameters *filter-id* — specifies the IPv6 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-name — A string of up to 64 characters uniquely identifying this IPv6 filter policy.

mac-filter

Syntax **mac-filter** *filter-id* [**create**]
mac-filter {*filter-id* | *filter-name*}
no mac-filter *filter-id*

Context config>filter

Description This command enables the context for a MAC filter policy.

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.

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

redirect-policy

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

Context config>filter

Description This command configures redirect policies.

The **no** form of the command removes the redirect policy from the filter configuration only if the policy is not referenced in an IP filter and the IP filter is not in use (applied to a service or network interface).

Default none

Parameters *redirect-policy-name* — Specifies the redirect policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. There is no limit to the number of redirect policies that can be configured.

log

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

Context config>filter

Description This command enables the context to create a filter log policy.

The **no** form of the command deletes the filter log ID. The log cannot be deleted if there are filter entries configured to write to the log. All filter entry logging associations need to be removed before the log can be deleted.

Special Cases **Filter log 101 —** Filter log 101 is the default log and is automatically created by the system. Filter log 101 is always a memory filter log and cannot be changed to a Syslog filter log. The log size defaults to 1000 entries. The number of entries and wrap-around behavior can be edited.

Default **log 101**

Parameters *log-id* — The filter log ID destination expressed as a decimal integer.

Values 101 — 199

DHCP Filter Commands

action

Syntax **action** {**bypass-host-creation**}
action drop
no action

Context config>filter>dhcp-filter>entry

Description This command specifies the action to take on DHCP host creation when the filter entry matches.

The **no** form of the command reverts to the default wherein the host creation proceeds as normal

Default no action

Parameters **bypass-host-creation —** Specifies that the host creation is bypassed.

drop — Specifies the DHCP message is dropped.

option

Syntax **option** *dhcp-option-number* {**present** | **absent**}
option *dhcp-option-number* **match hex** *hex-string* [**exact**] [**invert-match**]
option *dhcp-option-number* **match string** *ascii-string* [**exact**] [**invert-match**]
no option

Context config>filter>dhcp-filter>entry

Description This command configures the action to take on DHCP host creation when the filter entry matches.

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

Parameters *dhcp-option-number —*

Values 0 — 255

present — Specifies that the related DHCP option must be present.

absent — Specifies that the related DHCP option must be absent.

match hex *hex-string* — The option must (partially) match a specified hex string.

Values 0x0..0xFFFFFFFF...(max 254 hex nibbles)

match string *ascii-string* — The option must (partially) match a specified ASCII string.

Values Up to 127 characters

exact — This option requires an exact match of a hex or ascii string.

invert-match — Requires the option not to (partially) match.

Filter Log Commands

destination

Syntax **destination memory** *num-entries*
destination syslog *syslog-id*
no destination

Context config>filter>log

Description This command configures the destination for filter log entries for the filter log ID.

Filter logs can be sent to either memory (**memory**) or to an existing Syslog server definition (**server**).

If the filter log destination is **memory**, the maximum number of entries in the log must be specified.

The **no** form of the command deletes the filter log association.

Default **no destination**

Parameters **memory** *num-entries* — Specifies the destination of the filter log ID is a memory log. The *num-entries* value is the maximum number of entries in the filter log expressed as a decimal integer.

Values 10 — 50000

syslog *syslog-id* — Specifies the destination of the filter log ID is a Syslog server. The *syslog-id* parameter is the number of the Syslog server definition.

Values 1 — 10

shutdown

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

Context config>filter>log
config>filter>log>summary
config>filter>redirect-policy
config>filter>redirect-policy>destination

Administratively enables/disabled (AdminUp/AdminDown) an entity. Downing an entity does not change, reset or remove any configuration settings or statistics. Many objects must be shutdown before they may be deleted.

The **shutdown** command administratively downs an entity. Administratively downing an entity changes the operational state of the entity to down and the operational state of any entities contained within the administratively down entity.

Unlike other commands and parameters where the default state will not be 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

summary

Syntax **summary**

Context config>filter>log

Description This command enables the context to configure log summarization. These settings will only be taken into account when syslog is the log destination. Note that summary settings will only be taken into account in case the log destination is syslog.

Parameters none

summary-crit

Syntax **summary-crit dst-addr**
summary-crit src-addr
no summary-crit

Context config>filter>log>summary

Description This command defines the the key of the index of the minitable. If key information is changed while summary is in no shutdown, the filter summary minitable is flushed and recreated with different key information. Log packets received during the reconfiguration time will be handled as if summary was not active.

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

Default dst-addr

Parameters **dst-addr —** Specifies that received log packets are summarized based on the destination IP, IPv6, or MAC address.

src-addr — Specifies that received log packets are summarized based on the source IP, IPv6 or MAC address.

wrap-around

Syntax [**no**] **wrap-around**

Context config>filter>log

Description This command configures a memory filter log to log until full or to store the most recent log entries (circular buffer).

Specifying **wrap-around** configures the memory filter log to store the most recent filter log entries (circular buffer). When the log is full, the oldest filter log entries are overwritten with new entries.

The **no** form of the command configures the memory filter log to accept filter log entries until full. When the memory filter log is full, filter logging for the log filter ID ceases.

Default wrap-around

ACL Filter Policy Commands

default-action

Syntax **default-action** {**drop** | **forward**}

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

Description This command specifies the action to be applied to packets when the packets do not match the specified criteria in all of the IP filter entries of the filter.

When multiple **default-action** commands are entered, the last command will overwrite the previous command.

Default drop

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

forward — Specifies all packets will be forwarded unless there is a specific filter entry which causes the packet to be dropped.

embed-filter

Syntax **embed-filter** *filter-id* [**offset** *offset*] [{**active** | **inactive**}]
no embed-filter *filter-id*

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

Description This command embeds a previously defined IPv4, or IPv6 embedded filter policy into this exclusive or template filter policy at a specified offset value.

active | **inactive** keywords:

active – an embedded filter entries are to be included in this embedding filter policy and activated on applicable line cards – default if no keyword is specified and omitted in info command (but not info detail), or when saving configuration

inactive – an embedded filter policy entries are to be included in this embedded filter policy but are not downloaded to line cards – i.e. remain inactive. Always shown as part of info command or when saved to a configuration file.

The **no** form of this command removes the embedded filter policy from this filter policy.

Please see the description of embedded filter policies in this guide for further operational details.

Default No embedded filter policies are included in a filter policy by default

Parameters *filter-id* — Specifies a previously defined embedded filter policy.

offset — a value from 0 to 65535, an embedded filter entry X will have an entry X + offset in the embedding filter.

filter-name

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

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

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

Default no filter-name

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

scope

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

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

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

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

Default **template**

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

template — When the scope of a policy is defined as template, the policy can be applied to multiple SAPs or network ports.

embedded — When the scope of a policy is defined as embedded, the policy cannot be applied directly to SAP/interface. The policy defines embedded filter rules, which are embedded by other exclusive/template filter policies. embedded scope is supported for IP and IPv6 filter policies only.

shared-radius-filter-wmark

Syntax **shared-radius-filter-wmark low** *low-watermark* **high** *high-watermark*
no shared-radius-filter-wmark

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

Description This command configures the low and high watermark for the number of RADIUS shared filters reporting

Parameters **low** *low-watermark* — Specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be raised by the agent.

Values 0 — 8000

high *high-watermark* — Specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be cleared by the agent.

Values 1— 8000

sub-insert-credit-control

Syntax **sub-insert-credit-control start-entry** *entry-id* **count** *count*
no sub-insert-credit-control

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

Description This command inserts point information for credit control for the filter.

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

Default none

Parameters **entry** *entry-id* — Identifies a filter on this system.

Values 1 — 65535

count *count* — Specifies the count.

Values 1 — 65535

sub-insert-radius

Syntax **sub-insert-radius start-entry** *entry-id* **count** *count*
no sub-insert-radius

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

Description This command insert point information for RADIUS for the filter.

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

Default none

Parameters **entry** *entry-id* **—** Specifies at what place the filter entries received from RADIUS will be inserted in the filter.

Values 1 — 65535

count *count* **—** Specifies the count.

Values 1 — 65535

sub-insert-shared-radius

Syntax **sub-insert-shared-radius start-entry** *entry-id* **count c***ount*
no sub-insert-shared-radius

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

Description This command configures the insert point for shared host rules from RADIUS.

entry *entry-id* **—** Identifies a filter on this system.

Values 1 — 65535

count *count* **—** Specifies the count.

Values 1 — 65535

sub-insert-wmark

Syntax **sub-insert-wmark low** *low-watermark* **high** *high-watermark*
no sub-insert-wmark

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

Description This command configures the low and high watermark percentage for inserted filter entry usage reporting.

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

Default none

Parameters **low** *low-watermark* — Specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be cleared by the agent.

Values 0 — 100

high *high-watermark* — Specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be raised by the agent.

Values 0 — 100

type

Syntax **type** *filter-type*

Context config>filter>mac-filter

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

Default normal

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

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

General Filter Entry Commands

entry

Syntax **entry** *entry-id* [**time-range** *time-range-name*] [**create**]
no entry *entry-id*

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

Description This command creates or edits an IP (v4), IPv6, or MAC filter entry. Multiple entries can be created using unique entry-id numbers within the filter. Entries must be sequenced 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 filter. Entries removed from the filter are immidately 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.

log

Syntax **log** *log-id*
no log

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

Description This command creates the context to enable filter logging for a filter entry and specifies the

destination filter log ID.

The filter log ID must exist before a filter entry can be enabled to use the filter log ID.

The **no** form of the command disables logging for the filter entry.

Default **no log**

Parameters *log-id* — The filter log ID destination expressed as a decimal integer.

Values 101 — 199

IP (v4/v6) Filter Entry Commands

action

Syntax **action** [**drop**]
action forward [**next-hop** {*ip-address* | **indirect** *ip-address* | **interface** *ip-int-name*}]
action forward [**redirect-policy** *policy-name*]
action forward [**sap** *sap-id* | **sdp** s*dp-id:vc-id*]
action http-redirect *rdr-url-string*
action nat [*nat-policy-name*]
action reassemble
no action

Context config>filter>ip-filter>entry
config>filter>ipv6-filter>entry

Description This command specifies the action to take for packets that match this filter entry. The **action** command must be entered with a keyword specified in order for the entry to be active.

Note that **action forward next-hop** cannot be applied to multicast traffic.

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 **no action**

Parameters **drop** — Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded.

next-hop *ip-address* — The IP address of the direct next-hop to which to forward matching packets in dotted decimal notation.

indirect *ip-address* — The IP address of the indirect next-hop to which to forward matching packets in dotted decimal notation. The direct next-hop IP address and egress IP interface are determined by a route table lookup.

If the next hop is not available, then a routing lookup will be performed and if a match is found the packet will be forwarded to the result of that lookup. If no match is found a "ICMP destination unreachable" message is send back to the origin.

redirect *policy-name* — Specifies the redirect policy configured in the **config>filter>redirect-policy** context.

interface *ip-int-name* — The name of the egress IP interface where matching packets will be forwarded from. This parameter is only valid for unnumbered point-to-point interfaces. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

sap *sap-id* — Specifies the physical port identifier portion of the SAP definition. Only Ethernet SAPs are supported (including q-in-q, BCP, bridged Ethernet in Frame Relay or ATM).Refer to

Common CLI Command Descriptions on page 615 for SAP CLI command syntax and parameter descriptions.

sdp *sdp-id:vc-id* **—** specifies SDP defined in the system. now we need to reference to somewhere where SDP input is defined similarly to SAP reference above.

http-redirect *url* **—** Specifies the HTTP web address that will be sent to the user's browser. Note that http-redirect is not supported on 7750 SR-1 or 7450 ESS-1 models.

The following displays information that can optionally be added as variables in the portal URL (http-redirect url):

- $IP — Customer's IP address
- $MAC — Customer's MAC address
- $URL — Original requested URL
- $SAP — Customer's SAP
- $SUB — Customer's subscriber identification string"
- $SAPDESC — The description string configured on the SAP.
- $CID — A string that represents the circuit-id or interface-id of the subscriber host (hexadecimal format).
- $RID — A string that represents the remote-id of the subscriber host (hexadecimal format)

Values 255 characters maximum

router service-name *service-name* **—** Indicates the service id of the destination for this IP filter entry.

nat — specifyies that matching traffic is to be redirected for NAT performed by Integrated Service Adapter(s) running NAT application.

reassemble — Packets matching the filter entry are forwarded to the packet reassembly function in the system.

action

Syntax **action drop**
action forward
action forward next-hop [**ipv6-address** |**indirect ipv6-address**]
action nat [**nat-policy-name**]
action http-redirect url
no action

Context config>filter>ipv6-filter>entry

Description This command specifies the action to take for packets that match this filter entry. 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 **no action**

Parameters **drop —** Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded.

nat — specifyies that matching traffic is to be redirected for NAT performed by Integrated Service Adapter(s) running NAT application.

redirect *policy-name* **—** Specifies the redirect policy configured in the **config>filter>redirect-policy** context.

http-redirect *url* **—** Specifies the HTTP web address that will be sent to the user's browser. Note that http-redirect is not supported on 7750 SR-1 or 7450 ESS-1 models.

The following displays information that can optionally be added as variables in the portal URL (http-redirect url):

- $IP – Customer's IP address
- $MAC – Customer's MAC address
- $URL – Original requested URL
- $SAP – Customer's SAP
- $SUB – Customer's subscriber identification string"

Values 255 characters maximum

filter-sample

Syntax [**no**] **filter-sample**

Context config>filter>ip-filter>entry
config>filter>ipv6-filter>entry

Description Specifies that traffic matching the associated IP filter entry is sampled if the IP interface is set to **cflowd acl**.

If the cflowd is either not enabled or set to **cflowd interface** mode, this command is ignored.

The **no** form removes this command for the system configuration, disallowing the sampling of packets if the ingress interface is in **cflowd acl** mode.

Default **no filter-sample**

interface-disable-sample

Syntax [**no**] **interface-disable-sample**

Context config>filter>ip-filter>entry
config>filter>ipv6-filter>entry

Description This command specifies that traffic matching the associated IP filter entry is not sampled if the IP interface is set to **cflowd interface** mode. This allows the option to not sample specific types of traffic when interface sampling is enabled.

If the cflowd is either not enabled or set to **cflowd acl** mode, this command is ignored.

The **no** form of this command enables sampling.

Default no interface-disable-sample

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, hexidecimal, or binary - DHB)
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
* — udp/tcp wildcard

Protocol	Protocol ID	Description
icmp	1	Internet Control Message
igmp	2	Internet Group Management

Protocol	Protocol ID	Description
ip	4	IP in IP (encapsulation)
tcp	6	Transmission Control
egp	8	Exterior Gateway Protocol
igp	9	Any private interior gateway (used by Cisco for IGRP)
udp	17	User Datagram
rdp	27	Reliable Data Protocol
ipv6	41	IPv6
ipv6-route	43	Routing Header for IPv6
ipv6-frag	44	Fragment Header for IPv6
idrp	45	Inter-Domain Routing Protocol
rsvp	46	Reservation Protocol
gre	47	General Routing Encapsulation
ipv6-icmp	58	ICMP for IPv6
ipv6-no-nxt	59	No Next Header for IPv6
ipv6-opts	60	Destination Options for IPv6
iso-ip	80	ISO Internet Protocol
eigrp	88	EIGRP
ospf-igp	89	OSPFIGP
ether-ip	97	Ethernet-within-IP Encapsulation
encap	98	Encapsulation Header
pnni	102	PNNI over IP
pim	103	Protocol Independent Multicast
vrrp	112	Virtual Router Redundancy Protocol
l2tp	115	Layer Two Tunneling Protocol
stp	118	Spanning Tree Protocol
ptp	123	Performance Transparency Protocol
isis	124	ISIS over IPv4
crtp	126	Combat Radio Transport Protocol
crudp	127	Combat Radio User Datagram

match

Syntax **match** [**next-header** *next-header*]
no match

Context config>filter>ipv6-filter>entry

Description This command enables the context to enter match criteria for the 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 *next-header* — Specifies the IPv6 next header to match. Note that this parameter is analogous to the protocol parameter used in IP-Filter match criteria.

Values [0 — 42 | 45 — 49 | 52 — 59 | 61— 255] — protocol numbers accepted in decimal, hexidecimal, or binary - DHB
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
* — udp/tcp wildcard

Values

dscp

Syntax **dscp** *dscp-name*
no dscp

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion.

The **no** form of the command removes the DSCP match criterion.

Default **no dscp**

Parameters *dscp-name* — Configure a dscp name that has been previously mapped to a value using the **dscp-name** command. The DiffServ code point may only be specified by its name.

Values be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23

dst-ip

Syntax **dst-ip** {*ip-address*[*/mask*]} [*netmask* | **ip-prefix-list** *prefix-list-name*]
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

ip-prefix-list — creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ip-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

mask — The subnet mask length expressed as a decimal integer.

Values 1 — 32

netmask — Any mask epressed in dotted quad notation.

Values 0.0.0.0 — 255.255.255.255

dst-ip

Syntax **dst-ip** [*ipv6-address*/*prefix-length*|*ipv6-prefix-list/ipv6-prefix-list-name*]
no dst-ip

Context config>filter>ipv6-filter>entry>match

Description This command matches a destination IPv6 address.

To match on the destination IPv6 address, specify the address and prefix length, for example, 11::12/128.

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

Default none

Parameters *ipv6-prefix* — The IPv6 prefix for the IP match criterion in dotted decimal notation.

Values	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x::d.d.d.d x: [0..FFFF]H d: [0..255]D

prefix-length — The IPv6 prefix length for the ipv6-address expressed as a decimal integer.

Values 1 — 128

ipv6-prefix-list — creates a list of IPv6 prefixes for match criteria in IPv6 ACL and CPM filter policies.

ip-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

dst-port

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

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures a destination TCP or UDP port number or port range for an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

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

Default **none**

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

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

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

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

eq — Specifies the operator to use relative to *dst-port-number* for specifying the port number match criteria. The **eq** keyword specifies that *dst-port-number* must be an exact match.

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

Values 0 — 65535

range *start end* **—** Specifies an inclusive range of port numbers to be used as a match criteria. The destination port numbers *start-port* and *end-port* are expressed as decimal integers.

Values 0 — 65535

fragment

Syntax **fragment** {**true**|**false**|**first-only**|**non-first-only**}
no fragment

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command specifies fragmented or non-fragmented IP packets as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

This command enables match on existence of IPv6 Fragmentation Extension Header in the IPv6 filter policy. To match first fragment of an IP fragmented packet, specify additional Layer 4 matching criteria in a filter policy entry. The no version of this command ignores IPv6 Fragmentation Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

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

Default **no fragment**

Parameters **true —** Specifies to 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. For IPv6, packet matches if it contains IPv6 Fragmentation Extension Header.

false — Specifies to 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. For IPv6, packet matches if it does not contain IPv6 Fragmentation Extension Header.

first-only — Matches if a packet is an initial fragment of the fragmented IPv6 packet.

non-first-only — Matches if a packet is a non-initial fragment of the fragmented IPv6 packet.

ah-ext-hdr

ah-ext-hdr {**true**|**false** }
no ah-ext-hdr

Context config>filter>ipv6-filter>entry>match

Description This command enables match on existence of AH Extension Header in the IPv6 filter policy.

The **no** form of this command ignores AH Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default **no ah-ext-hdr**

Parameters **true** — Matches a packet with an AH Extension Header.

false — Match a packet without an AH Extension Header.

esp-ext-hdr

Syntax **esp-ext-hdr** {**true**|**false** }
no esp-ext-hdr

Context config>filter>ipv6-filter>entry>match

Description This command enables match on existence of ESP Extension Header in the IPv6 filter policy.

The **no** form of this command ignores ESP Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default **no esp-ext-hdr**

Parameters **true** — Matches a packet with an ESP Extension Header.

false — Match a packet without an ESP Extension Header.

hop-by-hop-opt

Syntax **hop-by-hop-opt** {**true**|**false**}
no hop-by-hop-opt

Context config>filter>ipv6-filter>entry>match

Description This command enables match on existence of Hop-by-Hop Options Extension Header in the IPv6 filter policy.

The **no** form of this command ignores Hop-by-Hop Options Extension Header presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default **hop-by-hop-opt**

Parameters **true —** Matches a packet *with* a Hop-by-hop Options Extensions header.

false — Matches a packet *without* a Hop-by-hop Options Extensions header.

icmp-code

Syntax **icmp-code** *icmp-code*
no icmp-code

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description Configures matching on ICMP/ICMPv6 code field in the ICMP/ICMPv6 header of an IP or IPv6 packet as a filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

This option is only meaningful if the protocol match criteria specifies ICMP (1).

The **no** form of the command removes the criterion from the match entry.

Default **no icmp-code**

Parameters *icmp-code* — The ICMP/ICMPv6 code values that must be present to match.

Values 0 — 255

icmp-type

Syntax **icmp-type** *icmp-type*
no icmp-type

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures matching on the ICMP/ICMPv6 type field in the ICMP/ICMPv6 header of an IP or IPv6 packet as a filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

This option is only meaningful if the protocol match criteria specifies ICMP (1).

The **no** form of the command removes the criterion from the match entry.

Default **no icmp-type**

Parameters *icmp-type* — The ICMP/ICMPv6 type values that must be present to match.

Values 0 — 255

ip-option

Syntax **ip-option** *ip-option-value* [*ip-option-mask*]
no ip-option

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

Description This command configures matching packets with a specific IP option or a range of IP options in the first option of the IP header as an IP filter match criterion.

The option-type octet contains 3 fields:

1 bit copied flag (copy options in all fragments)

2 bits option class

5 bits option number

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

Default none

Parameters *ip-option-value* — Enter the 8 bit option-type as a decimal integer. The mask is applied as an AND to the option byte, the result is compared with the option-value.

The decimal value entered for the match should be a combined value of the eight bit option type field and not just the option number. Thus to match on IP packets that contain the Router Alert option (option number = 20), enter the option type of 148 (10010100).

Values 0 — 255

ip-option-mask — This is optional and may be used when specifying a range of option numbers to use as the match criteria.

This 8 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	DDD	20
Hexadecimal	0xHH	0x14
Binary	0bBBBBBBBB	0b0010100

Default **255 (decimal) (exact match)**

Values 1 — 255 (decimal)

multiple-option

Syntax **multiple-option** {**true** | **false**}
no multiple-option

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

Description This command configures matching packets that contain one or more than one option fields in the IP header as an IP filter match criterion.

The **no** form of the command removes the checking of the number of option fields in the IP header as a match criterion.

Default **no multiple-option**

Parameters **true —** Specifies matching on IP packets that contain more than one option field in the header.

false — Specifies matching on IP packets that do not contain multiple option fields present in the header.

option-present

Syntax **option-present** {**true** | **false**}
no option-present

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

Description This command configures matching packets that contain the option field in the IP header as an IP filter match criterion.

The **no** form of the command removes the checking of the option field in the IP header as a match criterion.

Parameters **true —** Specifies matching on all IP packets that contain the option field in the header. A match will occur for all packets that have the option field present. An option field of zero is considered as no option present.

false — Specifies matching on IP packets that do not have any option field present in the IP header. (an option field of zero). An option field of zero is considered as no option present.

routing-type0

Syntax **routing-type0** {**true**|**false**}
no routing-type0

Context config>filter>ipv6-filter>entry>match

Description This command enables match on existence of Routing Type Extension Header type 0 in the IPv6 filter policy.

The **no** form of this command ignores Routing Type Extension Header type 0 presence/absence in a packet when evaluating match criteria of a given filter policy entry.

Default **no routing-type0**

Parameters **true** — match if a packet contains Routing Type Extension Header type 0

false — match if a packet does not contain Routing Type Extension Header type 0

src-ip

Syntax **src-ip** {*ip-address*[*/mask*]} [*netmask* | **ip-prefix-list** *prefix-list-name*]
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 **no src-ip**

Parameters *ip-address* — The valid IP prefix for the IP match criterion in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255

ip-prefix-list — creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

ip-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

mask — The subnet mask length expressed as a decimal integer.

Values 1 — 32

netmask — Any mask epressed in dotted quad notation.

Values 0.0.0.0 — 255.255.255.255

src-ip

Syntax **src-ip** [*ipv6-address*/*prefix-length*|*ipv6-prefix-list/ipv6-prefix-list-name*]
no src-ip

Context config>filter>ipv6-filter>entry>match

Description This command configures a source IPv6 address range to be used as an IP filter match criterion.

The **no** form of the command removes the source IPv6 address match criterion.

Default **no src-ip**

Parameters *ipv6-address* — The IP prefix for the IP match criterion in dotted decimal notation.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x [0..FFFF]H
d [0 — 255]D

prefix-length — The IPv6 mask value for the IPv6 filter entry.

Values 1 — 128

ipv6-prefix-list — creates a list of IPv6 prefixes for match criteria in IPv6 ACL and CPM filter policies.

ipv6-prefix-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

src-port

Syntax **src-port** {**lt** | **gt** | **eq**} *src-port-number*
src-port range *src-port-number src-port-number*
no src-port

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures a source TCP or UDP port number or port range for an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 information.

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

Default no src-port

Parameters **lt** | **gt** | **eq** — Specifies the operator to use relative to *src-port-number* for specifying the port number match criteria.

lt specifies all port numbers less than *src-port-number* match.

gt specifies all port numbers greater than *src-port-number* match.

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

src-port-number — The source port number to be used as a match criteria expressed as a decimal integer.

Values 0 — 65535

range *start end* — Specifies an inclusive range of port numbers to be used as a match criteria. The source port numbers *start-port* and *end-port* are expressed as decimal integers.

Values 0 — 65535

src-route-option

Syntax **src-route-option** {**true**|**false**}
no source-route-option

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

Description This command enables source route option match conditions. When enabled, this filter should match if a (strict or loose) source route option is present/not present at any location within the IP header, as per the value of this object.

Parameters **true** — Enables source route option match conditions.

false — Disables source route option match conditions.

tcp-ack

Syntax **tcp-ack** {**true** | **false**}
no tcp-ack

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures matching on the ACK bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first

fragment contains the Layer 4 information.

The **no** form of the command removes the criterion from the match entry.

Default no tcp-ack

Parameters **true —** Specifies matching on IP packets that have the ACK bit set in the control bits of the TCP header of an IP packet.

false — Specifies matching on IP packets that do not have the ACK bit set in the control bits of the TCP header of the IP packet.

tcp-syn

Syntax **tcp-syn** {**true** | **false**}
no tcp-syn

Context config>filter>ip-filter>entry>match
config>filter>ipv6-filter>entry>match

Description This command configures matching on the SYN bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion. Note that an entry containing Layer 4 match criteria will not match non-initial (2nd, 3rd, etc) fragments of a fragmented packet since only the first fragment contains the Layer 4 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.

Match List Configuration Commands

match-list

Syntax **match-list**

Context config>filter

Description This command enables the configuration context for match lists to be used in filter policies (IOM and CPM).

ip-prefix-list

Syntax **ip-prefix-list** *ip-prefix-list-name* **create**
no ip-prefix-list *ip-prefix-list-name*

Context config>filter>match-list

Description This command creates a list of IPv4 prefixes for match criteria in IPv4 ACL and CPM filter policies.

The **no** form of this command deletes the specified list.

Operational notes:

An **ip-prefix-list** must contain only IPv4 address prefixes.

An IPv4 prefix match list cannot be deleted if it is referenced by a filter policy.

Please see general description related to match-list usage in filter policies.

Default none

Parameters *ip-prefix-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

prefix

Syntax **prefix** *ip-prefix/prefix-length*
no prefix *ip-prefix/prefix-length*

Context config>filter>match-list>ip-prefix-list

Description This command adds an IPv4 address prefix to an existing IPv4 address prefix match list.

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

Operational notes:

To add set of unique prefixes, execute the command with all unique prefixes. The prefixes are allowed to overlap IPv4 address space.

An IPv4 prefix addition will be blocked, if resource exhaustion is detected anywhere in the system because of Filter Policies that use this IPv4 address prefix list.

Default none

Parameters *ip-prefix* — A valid IPv4 address prefix in dotted decimal notation.

Values 0.0.0.0 to 255.255.255.255 (host bit must be 0)

prefix-length — Length of the entered IP prefix.

Values 1 — 32

apply-path

Syntax **apply-path**
no apply-path

Context config>filter>match-list>ip-pfx-list
config>filter>match-list>ipv6-pfx-list

Description This command enables context to configure auto-generation of address prefixes for IPv4 or IPv6 address prefix match lists. The context the command is executed governs whether IPv4 or IPv6 prefixes will be auto-generated.

The **no** form of this command removes all auto-generation configuration under the apply-path context.

Default no apply path

bgp-peers

Syntax **bgp-peers** *index* **group** *reg-exp* **neighbor** *reg-exp*
no bgp-peers *index*

Context config>filter>match-list>ip-pfx-list>apply-path
config>filter>match-list>ipv6-pfx-list>apply-path

Description This command configures auto-generation of IPv4 or IPv6 address prefixes (as required by the context the command is executed within) based on the base router BGP instance configuration.

group:

Configures a match against base router BGP instance group configuration. Regex wildcard match (.*) can be used to match against any group.

neighbor:

Configures a match against base router BGP instance neighbor configuration. Regex wildcard match (.*) can be used to match against any neighbor.

The **no** form of this command removes the bgp-peers configuration for auto-generation of address prefixes for the specified index value.

Default No embedded filter policies are included in a filter policy.

Parameters *index* — An integer from 1 to 255 enumerating bgp-peers auto-generation configuration within this list.

reg-exp — A regular expression defining a macth string to be used to auto generate address prefixes. Matching is performed from the least significant digit. For example a string **10.0** matches all neighbors with addresses starting with **10**; like **10.0.x.x** or **10.0xx.x.x**.

ipv6-prefix-list

Syntax **ipv6-prefix-list** *ipv6-prefix-list-name* **create**
no ipv6-prefix-list i*pv6-prefix-list-name*

Context config>filter>match-list

Description This command creates a list of IPv6 prefixes for match criteria in ACL and CPM IPv6 filter policies.

The **no** form of this command deletes the specified list.

Operational notes:

An **ipv6-prefix-list** must contain only IPv6 address prefixes.

An IPv6 prefix match list cannot be deleted if it is referenced by a filter policy.

Please see general description related to match-list usage in filter policies.

Parameters *ipv6-prefix-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

port-list

Syntax **port-list** *port-list-name* **create**
no port-list *port-list-name*

Context config>filter>match-list

Description This command creates a list of TCP/UDP port values or ranges for match criteria in IPv4 and IPv6 ACL and CPM filter policies.

The **no** form of this command deletes the specified list.

Operational notes:

A port-list must contain only TCP/UDP port values or ranges.

A TCP/UDP port match list cannot be deleted if it is referenced by a filter policy.

Please see general description related to match-list usage in filter policies.

Parameters *port-list-name* — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

Default no ports are added to a port list by default.

prefix

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

Context config>filter>match-list>ipv6>pfx>list

Description This command adds an IPv6 address prefix to an existing IPv6 address prefix match list.

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

Operational notes:

To add set of different prefixes, execute the command with all unique prefixes. The prefixes are allowed to overlap IPv6 address space.

An IPv6 prefix addition will be blocked, if resource exhaustion is detected anywhere in the system because of Filter Policies that use this IPv6 address prefix list.

Default No prefixes are in the list by default

Parameters *ipv6-prefix* — A An IPv6 address prefix written as hexadecimal numbers separated by colons with host bits set to 0. One string of zeros can be omitted so 1010::700:0:217A is equivalent to 1010:0:0:0:0:700:0:217A

Values ipv6-prefix: - IPv6 address prefix
x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D

prefix-length — Length of the entered IP prefix.

Values 1 — 128

Parameters *port-number* — A source or destination port to be used as a match criterion specified as a decimal integer.

Values 1 -65535

range *start end* — an inclusive range of source or destination port values to be used as match criteria. *start* of the range and *end* of the range are expressed as decimal integers.

Values 1 -65535

port-list-name — A string of up to 32 characters of printable ASCII characters. If special characters are used, the string must be enclosed within double quotes.

MAC Filter Entry Commands

action

Syntax **action drop**
action forward [**sap** *sap-id* |**sdp** *sdp-id*]
no action

Context config>filter>mac-filter>entry

Description This command configures the action for a MAC filter entry. The **action** keyword must be entered for the entry to be active. Any filter entry without the **action** keyword will be considered incomplete and will be inactive.

If neither drop nor forward is specified, this is considered a No-Op filter entry used to explicitly set a filter entry inactive without modifying match criteria or removing the entry itself.

Multiple action statements entered will overwrite previous actions parameters when defined. To remove a parameter, use the no form of the action command with the specified parameter.

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

Default none

Parameters **drop** — Specifies packets matching the entry criteria will be dropped.

forward — Specifies packets matching the entry criteria will be forwarded. Only Ethernet SAPs are supported (including q-in-q, BCP, bridged Ethernet in Frame Relay or ATM).

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

sap *sap-id* — Specifies the physical port identifier portion of the SAP definition. Refer to Common CLI Command Descriptions on page 615 for SAP CLI command syntax and parameter descriptions.

match

Syntax **match** [**frame-type 802dot3** | **802dot2-llc** | **802dot2-snap** | **ethernet_II**]
no match

Context config>filter>mac-filter>entry

Description This command creates the context for entering/editing match criteria for the filter entry and specifies an Ethernet frame type for the entry. When the match criteria have been satisfied the action associated with the match criteria is executed.

If more than one match criteria (within one match statement) are configured then all criteria must be satisfied (AND function) before the action associated with the match will be executed.

A **match** context may consist of multiple match criteria, but multiple **match** statements cannot be

entered per entry.

The **no** form of the command removes the match criteria for the *entry-id*.

Parameters **frame-type** *keyword* **—** The **frame-type** keyword configures an Ethernet frame type to be used for the MAC filter match criteria.

Default **802dot3ethernet_II**

Values 802dot3, 802dot2-llc, 802dot2-snap, ethernet_II

802dot3 — Specifies the frame type is Ethernet IEEE 802.3.

802dot2-llc — Specifies the frame type is Ethernet IEEE 802.2 LLC.

802dot2-snap — Specifies the frame type is Ethernet IEEE 802.2 SNAP.

ethernet_II — Specifies the frame type is Ethernet Type II.

MAC Filter Match Criteria

dot1p

Syntax **dot1p** *ip-value* [*mask*]
no dot1p

Context config>filter>mac-filter>entry

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.

SAP Egress

Egress **dot1p** value matching will only match if the customer payload contains the 802.1p bits. For example, if a packet ingresses on a null encapsulated SAP and the customer packet is IEEE 802.1Q or 802.1p tagged, the 802.1p bits will be present for a match evaluation. On the other hand, if a customer tagged frame is received on a dot1p encapsulated SAP, the tag will be stripped on ingress and there will be no 802.1p bits for a MAC filter match evaluation; in this case, any filter entry with a dot1p match criterion specified will fail.

Default no dot1p

Parameters *ip-value* — The IEEE 802.1p value in decimal.

Values 0 — 7

mask — This 3-bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	D	4
Hexadecimal	0xH	0x4
Binary	0bBBB	0b100

To select a range from 4 up to 7 specify *p-value* of 4 and a *mask* of 0b100 for value and mask.

Default **7 (decimal)**

Values 1 — 7 (decimal)

dsap

Syntax **dsap** *dsap-value* [*mask*]
no dsap

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

Description Configures an Ethernet 802.2 LLC DSAP value or range for a MAC filter match criterion.

This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. MAC Match Criteria Exclusivity Rules on page 419 describes fields that are exclusive based on the frame format.

Use the **no** form of the command to remove the dsap value as the match criterion.

Default no dsap

Parameters *dsap-value* — The 8-bit dsap match criteria value in hexadecimal.

Values 0x00 — 0xFF (hex)

mask — This is optional and may be used when specifying a range of dsap values to use as the match criteria.

This 8 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	DDD	240
Hexadecimal	0xHH	0xF0
Binary	0bBBBBBBBB	0b11110000

Default **FF (hex) (exact match)**

0x00 — 0xFF

dst-mac

Syntax **dst-mac** *ieee-address* [*mask*]
no dst-mac

Context config>filter>mac-filter>entry

Description Configures a destination MAC address or range to be used as a MAC filter match criterion.

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

Default no dst-mac

Parameters *ieee-address* — The MAC address to be used as a match criterion.

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

mask — A 48-bit mask to match a range of MAC address values.

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

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0xFFFFFF000000
Binary	0bBBBBBBBB...B	0b11110000...B

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 0003FA000000 0x0FFFFF000000

Default **0xFFFFFFFFFFFF (exact match)**

Values 0x00000000000000 — 0xFFFFFFFFFFFF

etype

Syntax **etype** *ethernet-type*
no etype

Context config>filter>mac-filter>entry

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. For IEEE 802.3 frames, use the dsap, ssap or snap-pid fields as match criteria.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. Table 11, MAC Match Criteria Exclusivity Rules, on page 419describes fields that are exclusive based on the frame format.

The **no** form of the command removes the previously entered etype field as the match criteria.

Default no etype

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

Values 0x0600 — 0xFFFF

isid

Syntax **isid** *value* [**to** *higher-value*]
no isid

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

Description This command configures an ISID value or a range of ISID values to be matched by the mac-filter parent. The pbb-etype value for the related SAP (inherited from the ethernet port configuration) or for the related SDP binding (inherited from SDP configuration) will be used to identify the ISID tag. When an isid statement is used in a match criteria the corresponding mac-filter can be applied only on the egress side of a SAP/SDP binding. In order to be able to use an isid match criteria one needs to set the mac-filter type attribute to isid. Once this configuration is performed only ISID match criteria are allowed in the mac-filter.

The **no** form of this command removes the ISID match criterion.

Default no isid

value — Specifies the ISID value, 24 bits. When just one present identifies a particular ISID to be used for matching.

to *higher-value* — Identifies a range of ISIDs to be used as matching criteria.

inner-tag

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

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

Description This command configures the matching of the second tag that is carried transparently through the service. The inner-tag on ingress is the second tag on the frame if there are no service delimiting tags. Inner tag is the second tag before any service delimiting tags on egress but is dependent in the ingress configuration and may be set to 0 even in cases where additional tags are on the frame. This allows matching VLAN tags for explicit filtering or QoS setting when using default or null encapsulations.

The inner-tag is not applicable in ingress on dot1Q SAPs. The inner-tag may be populated on egress depending on the ingress SAP type.

On QinQ SAPs of null and default that do not strip tags inner-tag will contain the second tag (which is still the second tag carried transparently through the service.) On ingress SAPs that strip any tags, inner-tag will contain 0 even if there are more than 2 tags on the frame.

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

Note for QoS the VID type cannot be specified on the default QoS policy.

The default vid-mask is set to 4095 for exact match.

outer-tag

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

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

Description This command configures the matching of the first tag that is carried transparently through the service. Service delimiting tags are stripped from the frame and outer tag on ingress is the first tag after any service delimiting tags. Outer tag is the first tag before any service delimiting tags on egress. This allows matching VLAN tags for explicit filtering or QoS setting when using default or null encapsulations.

On dot1Q SAPs outer-tag is the only tag that can be matched. On dot1Q SAPs with exact match (sap 2/1/1:50) the outer-tag will be populated with the next tag that is carried transparently through the service or 0 if there is no additional VLAN tags on the frame.

On QinQ SAPs that strip a single service delimiting tag, outer-tag will contain the next tag (which is still the first tag carried transparently through the service.) On SAPs with two service delimiting tags (two tags stripped) outer-tag will contain 0 even if there are more than 2 tags on the frame.

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

Note for QoS the VID type cannot be specified on the default QoS policy.

The default vid-mask is set to 4095 for exact match.

snap-oui

Syntax **snap-oui** [**zero** | **non-zero**]
no snap-oui

Context config>filter>mac-filter>entry

Description This command configures an IEEE 802.3 LLC SNAP Ethernet Frame OUI zero or non-zero value to be used as a MAC filter match criterion.

The **no** form of the command removes the criterion from the match criteria.

Default no snap-oui

Parameters **zero —** Specifies to match packets with the three-byte OUI field in the SNAP-ID set to zero.

non-zero — Specifies to match packets with the three-byte OUI field in the SNAP-ID not set to zero.

snap-pid

Syntax **snap-pid** *pid-value*
no snap-pid

Context config>filter>mac-filter>entry

Description Configures an IEEE 802.3 LLC SNAP Ethernet Frame PID value to be used as a MAC filter match criterion.

This is a two-byte protocol id that is part of the IEEE 802.3 LLC SNAP Ethernet Frame that follows the three-byte OUI field.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. MAC Match Criteria Exclusivity Rules on page 419 describes fields that are exclusive based on the frame format.

Note: The snap-pid match criterion is independent of the OUI field within the SNAP header. Two packets with different three-byte OUI fields but the same PID field will both match the same filter entry based on a snap-pid match criteria.

The **no** form of the command removes the snap-pid value as the match criteria.

Default no snap-pid

Parameters *pid-value* — The two-byte snap-pid value to be used as a match criterion in hexadecimal.

Values 0x0000 — 0xFFFF

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context config>filter>mac-filter>entry

Description Configures a source MAC address or range to be used as a MAC filter match criterion.

The **no** form of the command removes the source mac as the match criteria.

Default no src-mac

Parameters *ieee-address* — Enter the 48-bit IEEE mac address to be used as a match criterion.

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

ieee-address-mask — This 48-bit mask can be configured using:

Format Style	Format Syntax	Example
Decimal	DDDDDDDDDDDDD	281474959933440
Hexadecimal	0xHHHHHHHHHHHH	0x0FFFFF000000

Format Style	Format Syntax	Example
Binary	0bBBBBBBB...B	0b11110000...B

To configure so that all packets with a source MAC OUI value of 00-03-FA are subject to a match condition then the entry should be specified as: 003FA000000 0xFFFFFF000000

Default **0xFFFFFFFFFFFF** (exact match)

Values 0x00000000000000 — 0xFFFFFFFFFFFF

ssap

Syntax **ssap** *ssap-value* [*ssap-mask*]
no ssap

Context config>filter>mac-filter>entry

Description This command configures an Ethernet 802.2 LLC SSAP value or range for a MAC filter match criterion.

This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and may not be part of the same match criteria. MAC Match Criteria Exclusivity Rules on page 419 describes fields that are exclusive based on the frame format.

The **no** form of the command removes the ssap match criterion.

Default no ssap

Parameters *ssap-value* — The 8-bit ssap match criteria value in hex.

Values 0x00 — 0xFF

ssap-mask — This is optional and may be used when specifying a range of ssap values to use as the match criteria.

This 8 bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	DDD	240
Hexadecimal	0xHH	0xF0
Binary	0bBBBBBBBB	0b11110000

Default **none**

Values 0x00 — 0xFF

Policy and Entry Maintenance Commands

copy

Syntax **copy ip-filter src-filter-id [src-entry src-entry-id] to dst-filter-id [dst-entry dst-entry-id] [overwrite]**
copy ipv6-filter *src-filter-id* [**src-entry** *src-entry-id*] **to** *dst-filter-id* [dst-entry *dst-entry-id*] [**overwrite**]
copy mac-filter *src-filter-id* [**src-entry** *src-entry-id*] **to** *dst-filter-id* [dst-entry *dst-entry-id*] [**overwrite**]

Context config>filter

Description This command copies existing filter list entries for a specific filter ID to another filter ID. The **copy** command is a configuration level maintenance tool used to create new filters using existing filters. It also allows bulk modifications to an existing policy with the use of the **overwrite** keyword.
If **overwrite** is not specified, an error will occur if the destination policy ID exists.

Parameters **ip-filter —** Indicates that the *source-filter-id* and the *dest-filter-id* are IP filter IDs.

ipv6-filter — This keyword indicates that the *source-filter-id* and the *dest-filter-id* are IPv6 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**, **ipv6-filter** or **mac-filter**).

dest-filter-id — The *dest-filter-id* identifies the destination filter policy to which the copy command will attempt to copy. If the **overwrite** keyword does not follow, the filter policy ID cannot already exist within the system for the filter type the copy command is issued for. If the **overwrite** keyword is present, the destination policy ID may or may not exist.

overwrite — The **overwrite** keyword specifies that the destination filter ID may exist. If it does, everything in the existing destination filter ID will be completely overwritten with the contents of the source filter ID. If the destination filter ID exists, either **overwrite** must be specified or an error message will be returned. If **overwrite** is specified, the function of copying from source to destination occurs in a 'break before make' manner and therefore should be handled with care.

filter-name

Syntax **filter-name** *filter-name*
no filter-name

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

Description This command specifies the name to associate with this filter.

Parameters *filter-name* — Specifies the filter name up to 64 characters in length.

group-inserted-entries

Syntax **group-inserted-entries application** *application* **location** *location*

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

Description This command groups filter entries that are inserted in a filter by either RADIUS or Credit Control.

Parameters **application** *application* **—** Specifies for which application the the inserted entries must be grouped.

Values radius, credit-control

location *location* **—** Specifies at what location the inserted entries must be grouped.

Values top, bottom

renum

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

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

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

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

Values 1 — 65535

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

Values 1 — 65535

Redirect Policy Commands

destination

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

Context config>filter>redirect-policy

Description This command defines a cache server destination in a redirect policy. More than one destination can be configured. Whether a destination IP address will receive redirected packets depends on the effective priority value after evaluation.

Default none

Parameters *ip-address* — Specifies the IP address to send the redirected traffic.

ping-test

Syntax [**no**] **ping-test**

Context config>filter>destination>ping-test
config>filter>destination>snmp-test

Description This command configures parameters to perform connectivity ping tests to validate the ability for the destination to receive redirected traffic.

Default none

drop-count

Syntax **drop-count** *consecutive-failures* [**hold-down** *seconds*]
no drop-count

Context config>filter>destination>ping-test
config>filter>destination>snmp-test
config>filter>destination>url-test

Description This command specifies the number of consecutive requests that must fail for the destination to be declared unreachable.

Default drop-count 3 hold-down 0

Parameters *consecutive-failures* — Specifies the number of consecutive ping test failures before declaring the destination down.

Values 1 — 60

hold-down *seconds* — The amount of time, in seconds, that the system should be held down if any of the test has marked it unreachable.

Values 0 — 86400

interval

Syntax **interval** *seconds*
no interval

Context config>filter>destination>ping-test
config>filter>destination>snmp-test
config>filter>destination>url-test

Description This command specifies the amount of time, in seconds, between consecutive requests sent to the far end host.

Default 1

Parameters *seconds* — Specifies the amount of time, in seconds, between consecutive requests sent to the far end host.

Values 1 — 60

timeout

Syntax **timeout** *seconds*
no timeout

Context config>filter>destination>snmp-test
config>filter>destination>url-test

Description Specifies the amount of time, in seconds, that is allowed for receiving a response from the far-end host. If a reply is not received within this time the far-end host is considered unresponsive.

Default 1

Parameters *seconds* — Specifies the amount of time, in seconds, that is allowed for receiving a response from the far end host.

Values 1 — 60

priority

Syntax **priority** *priority*
no priority

Context config>filter>destination

Description Redirect policies can contain multiple destinations. Each destination is assigned an initial or base **priority** which describes its relative importance within the policy. If more than one destination is specified, the destination with the highest effective priority value is selected.

Default 100

Parameters *priority* — The priority, expressed as a decimal integer, used to weigh the destination's relative importance within the policy.

Values 1 — 255

snmp-test

Syntax **snmp-test** *test-name*

Context config>filter>redirect-policy>destination

Description This command enables the context to configure SNMP test parameters.

Default none

Parameters *test-name* — specifies the name of the SNMP test. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

oid

Syntax **oid** *oid-string* **community** *community-string*

Context config>filter>redirect-policy>destination>snmp-test

Description This command specifies the OID of the object to be fetched from the destination.

Default none

Parameters *oid-string* — Specifies the object identifier (OID) in the OID field.

community *community-string* — The SNMP v2 community string or the SNMP v3 context name used to conduct this SNMP test.

return-value

Syntax **return-value** *return-value* **type** *return-type* [**disable** | **lower-priority** *priority* | **raise-priority** *priority*]

Context config>filter>redirect-policy>destination>snmp-test

Description This command specifies the criterion to adjust the priority based on the test result. Multiple criteria can be specified with the condition that they are not conflicting or overlap. If the returned value is

within the specified range, the priority can be disabled, lowered or raised.

Default none

Parameters *return-value* — Specifies the SNMP value against which the test result is matched.

Values A maximum of 256 characters.

return-type — Specifies the SNMP object type against which the test result is matched.

Values integer, unsigned, string, ip-address, counter, time-ticks, opaque

disable — The keyword that specifies that the destination may not be used for the amount of time specified in the hold-time command when the test result matches the criterion.

lower-priority *priority* **—** Specifies the amount to lower the priority of the destination.

Values 1 — 255

raise-priority *priority* **—** Specifies the amount to raise the priority of the destination.

Values 1 — 255

url-test

Syntax **url-test** *test-name*

Context config>filter>redirect-policy>destination

Description The context to enable URL test parameters. IP filters can be used to selectively cache some web sites.

Default none

Parameters **test-name —** The name of the URL test. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

return-code

Syntax **return-code** *return-code-1* [*return-code-2*] [**disable** | **lower-priority** *priority* | **raise-priority** *priority*]
no return-code *return-code-1* [*return-code-2*]

Context config>filter>redirect-policy>destination>url-test

Description Return codes are returned when the URL test is performed. Values for the specified range are the return codes which can be given back to the system as a result of the test been performed.

For example, error code 401 for HTTP is “page not found.” If, while performing this test, the URL is not reachable, you can lower the priority by 10 points so that other means of reaching this destination are prioritized higher than the older one.

Default none

Parameters *return-code-1, return-code-2* — Specifies a range of return codes. When the URL test return-code falls within the specified range, the corresponding action is performed.

Values *return-code-1*: 1 — 4294967294
return-code-2: 2 — 4294967295

disable — Specifies that the destination may not be used for the amount of time specified in the hold-time command when the return code falls within the specified range.

lower-priority *priority* — Specifies the amount to lower the priority of the destination when the return code falls within the specified range.

raise-priority *priority* — Specifies the amount to raise the priority of the destination when the return code falls within the specified range.

url

Syntax **url** *url-string* [**http-version** *version-string*]

Context config>filter>redirect-policy>destination>url-test

Description This command specifies the URL to be probed by the URL test.

Default none

Parameters *url-string* — Specify a URL up to 255 characters in length.

http-version *version-string* — Specifies the HTTP version, 80 characters in length.