Show Commands

dhcp

Syntax **dhcp** [*filter-id*]

Context show>filter

Description This command displays DHCP filter information.

```
*B:TechPubs>config# show filter dhcp
===============================================================================
DHCP Filters
===============================================================================
Filter-Id   Applied Description
-------------------------------------------------------------------------------
10          No      test-dhcp-filter
-------------------------------------------------------------------------------
Num filter entries: 1
===============================================================================
*B:TechPubs>config#


*B:TechPubs>config# show filter dhcp 10
===============================================================================
DHCP Filter
===============================================================================
Filter-Id    : 10                       Applied      : No
Entries      : 0
Description  : test-dhcp-filter
-------------------------------------------------------------------------------
Filter Match Criteria
-------------------------------------------------------------------------------
No Match Criteria Found
===============================================================================
*B:TechPubs>config#
```

download-failed

Syntax **download-failed**

Context show>filter

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

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

Label	Description
Filter-type	Displays the filter type.
Filter-ID	Displays the ID of the filter.
Filter-Entry	Displays the entry number of the filter.

Sample Output

```
A:ALA-48# show filter download-failed
===============================================
Filter entries for which download failed
===============================================
Filter-type    Filter-Id      Filter-Entry
-----------------------------------------------
ip              1          10
===============================================
A:ALA-48#
```

ip

Syntax **ip**
ip embedded [**inactive**]
ip *ip-filter-id* **embedded** [**inactive**]
ip *ip-filter-id* [**detail**]
ip *ip-filter-id* **associations**
ip *ip-filter-id* **type** *entry-type*
ip *ip-filter-id* **counters** [**type** *entry-type*]
ip *ip-filter-id* **entry** *entry-id* **counters**
ip *ip-filter-id* **entry** *entry-id* [**detail**]

Context show>filter

Description This command shows IP filter information.

Parameters *ip-filter-id* — Displays detailed information for the specified filter ID and its filter entries.

Values 1 — 65535

entry *entry-id* **—** Displays information on the specified filter entry ID for the specified filter ID only.

Values 1 — 65535

associations — Appends information as to where the filter policy ID is applied to the detailed filter policy ID output.

counters — Displays counter information for the specified filter ID. Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.

type *entry-type* — specifies type of filter entry to display, values:

Values fixed, radius-insert, credit-control-insert, flowspec, embedded, radius-shared

embedded [**failed**] — Shows all embeddings, optionally shows failed embedding only, if *filter-id* is not specified shows all embedded filters.

Output **Show Filter (no filter-id specified) —** The following table describes the command output for the command when no filter ID is specified.

Label	Description
Filter Id	The IP filter ID
Scope	Template – The filter policy is of type template. Exclusive – The filter policy is of type exclusive.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Description	The IP filter policy description.
In	Shows embedding filter index
From	Shows embedded filters included
Priority	Shows priority of embedded filter
Inserted	Shows embedded/total number of entries from embedded filter Status: **OK**—embedding operation successful, if any entries are overwritten this will also be indicated. **Failed**—embedding failed, the reason is displayed (out of resources).

Sample Output

```
A:ALA-49# show filter ip
===============================================================================
IP Filters
===============================================================================
Filter-Id Scope    Applied Description
-------------------------------------------------------------------------------
1         Template Yes
3         Template Yes
6         Template Yes
10        Template No
11        Template No
-------------------------------------------------------------------------------
Num IP filters: 5
===============================================================================
A:ALA-49#

*A:Dut-C>config>filter# show filter ip
```

```
===============================================================================
IP Filters                                                        Total:     2
===============================================================================
Filter-Id   Scope    Applied Description
-------------------------------------------------------------------------------
10001       Template Yes
fSpec-1     Template Yes     BGP FlowSpec filter for the Base router
-------------------------------------------------------------------------------
Num IP filters: 2
===============================================================================
*A:Dut-C>config>filter# show filter ip embedded
================================================
IP Filter embedding
================================================
In       From    Priority   Inserted    Status
-------------------------------------------------------------------------------
10       2         50        1/1         OK
         1         100       1/2         OK- 1 entry overwritten

20       2         100       0/5         Failed - out of resources
================================================
*A:Dut-C>config>filter#
```

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

Label	Description
Filter Id	The IP filter policy ID.
Scope	Template – The filter policy is of type template. Exclusive – The filter policy is of type exclusive.
Entries	The number of entries configured in this filter ID.
Description	The IP filter policy description.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward. Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	IP – Indicates the filter is an IP filter policy.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
Log Id	The filter log ID.
Src. IP	The source IPv6 address and prefix length match criterion.

Label	Description (Continued)
Dest. IP	The destination IPv6 address and prefix length match criterion.
Next-header	The next header ID for the match criteria. Undefined indicates no next-header specified.
ICMP Type	The ICMP type match criterion. Undefined indicates no ICMP type specified.
Fragment	False – Configures a match on all non-fragmented IP packets. True – Configures a match on all fragmented IP packets. Off – Fragments are not a matching criteria. All fragments and non-fragments implicitly match.
Sampling	Off – Specifies that traffic sampling is disabled. On – Specifies that traffic matching the associated IP filter entry is sampled.
IP-Option	Specifies matching packets with a specific IP option or a range of IP options in the IP header for IP filter match criteria.
TCP-syn	False – Configures a match on packets with the SYN flag set to false. True – Configured a match on packets with the SYN flag set to true. Off – The state of the TCP SYN flag is not considered as part of the match criteria.
Match action	Default – The filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete, no action was specified. Drop – Drop packets matching the filter entry. Forward – The explicit action to perform is forwarding of the packet.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Src. Port	The source TCP or UDP port number or port range.
Dest. Port	The destination TCP or UDP port number or port rangee.
Dscp	The DiffServ Code Point (DSCP) name.
ICMP Code	The ICMP code field in the ICMP header of an IP packet.
Option-present	Off – Specifies not to search for packets that contain the option field or have an option field of zero.

Label	Description (Continued)
	On – Matches packets that contain the option field or have an option field of zero be used as IP filter match criteria.
Int. Sampling	Off – Interface traffic sampling is disabled.
	On – Interface traffic sampling is enabled.
Multiple Option	Off – The option fields are not checked.
	On – Packets containing one or more option fields in the IP header will be used as IP filter match criteria.
TCP-ack	False – Configures a match on packets with the ACK flag set to false.
	True – Configurs a match on packets with the ACK flag set to true.
	Off – The state of the TCP ACK flag is not considered as part of the match criteria. as part of the match criteria.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

Sample Output

```
A:ALA-49>config>filter# show filter ip 3
===============================================================================
IP Filter
===============================================================================
Filter Id    : 3                                Applied        : Yes
Scope        : Template                         Def. Action    : Drop
Entries      : 1
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry        : 10
Log Id       : n/a
Src. IP      : 10.1.1.1/24                      Src. Port      : None
Dest. IP     : 0.0.0.0/0                        Dest. Port     : None
Protocol     : 2                                Dscp           : Undefined
ICMP Type    : Undefined                        ICMP Code      : Undefined
TCP-syn      : Off                              TCP-ack        : Off
Match action : Drop
Ing. Matches : 0                                Egr. Matches   : 0
===============================================================================
A:ALA-49>config>filter#

*A:Dut-C>config>filter# show filter ip fSpec-1 associations
===============================================================================
IP Filter
===============================================================================
Filter Id    : fSpec-1                          Applied        : Yes
Scope        : Template                         Def. Action    : Forward
Radius Ins Pt: n/a
CrCtl. Ins Pt: n/a
Entries      : 2 (insert By Bgp)
```

```
Description  : BGP FlowSpec filter for the Base router
-------------------------------------------------------------------------------
Filter Association : IP
-------------------------------------------------------------------------------
Service Id   : 1                                  Type           : IES
- SAP    1/1/3:1.1   (merged in ip-fltr 10001)
===============================================================================
*A:Dut-C>config>filter#


*A:Dut-C>config>filter# show filter ip 10001
===============================================================================
IP Filter
===============================================================================
Filter Id    : 10001                              Applied        : Yes
Scope        : Template                           Def. Action    : Drop
Radius Ins Pt: n/a
CrCtl. Ins Pt: n/a
Entries      : 1
BGP Entries  : 2
Description  : (Not Specified)
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry        : 1
Description  : (Not Specified)
Log Id       : n/a
Src. IP      : 0.0.0.0/0                          Src. Port      : None
Dest. IP     : 0.0.0.0/0                          Dest. Port     : None
Protocol     : 6                                  Dscp           : Undefined
ICMP Type    : Undefined                          ICMP Code      : Undefined
Fragment     : Off                                Option-present : Off
Sampling     : Off                                Int. Sampling  : On
IP-Option    : 0/0                                Multiple Option: Off
TCP-syn      : Off                                TCP-ack        : Off
Match action : Forward
Next Hop     : Not Specified
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

Entry        : fSpec-1-32767  - inserted by BGP FLowSpec
Description  : (Not Specified)
Log Id       : n/a
Src. IP      : 0.0.0.0/0                          Src. Port      : None
Dest. IP     : 0.0.0.0/0                          Dest. Port     : None
Protocol     : 6                                  Dscp           : Undefined
ICMP Type    : Undefined                          ICMP Code      : Undefined
Fragment     : Off                                Option-present : Off
Sampling     : Off                                Int. Sampling  : On
IP-Option    : 0/0                                Multiple Option: Off
TCP-syn      : Off                                TCP-ack        : Off
Match action : Drop
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

Entry        : fSpec-1-49151  - inserted by BGP FLowSpec
Description  : (Not Specified)
Log Id       : n/a
Src. IP      : 0.0.0.0/0                          Src. Port      : None
```

```
Dest. IP     : 0.0.0.0/0                        Dest. Port     : None
Protocol     : 17                               Dscp           : Undefined
ICMP Type    : Undefined                        ICMP Code      : Undefined
Fragment     : Off                              Option-present : Off
Sampling     : Off                              Int. Sampling  : On
IP-Option    : 0/0                              Multiple Option: Off
TCP-syn      : Off                              TCP-ack        : Off
Match action : Drop
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

===============================================================================
*A:Dut-C>config>filter#
```

Output **Show Filter (with time-range specified) —** If a time-range is specified for a filter entry, the following is displayed.

```
A:ALA-49# show filter ip  10
===============================================================================
IP Filter
===============================================================================
Filter Id    : 10                               Applied        : No
Scope        : Template                         Def. Action    : Drop
Entries      : 2
-------------------------------------------------------------------------------
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry        : 1010
time-range   : day                              Cur. Status    : Inactive
Log Id       : n/a
Src. IP      : 0.0.0.0/0                        Src. Port      : None
Dest. IP     : 10.10.100.1/24                   Dest. Port     : None
Protocol     : Undefined                        Dscp           : Undefined
ICMP Type    : Undefined                        ICMP Code      : Undefined
Fragment     : Off                              Option-present : Off
Sampling     : Off                              Int. Sampling  : On
IP-Option    : 0/0                              Multiple Option: Off
TCP-syn      : Off                              TCP-ack        : Off
Match action : Forward
Next Hop     : 138.203.228.28
Ing. Matches : 0                                Egr. Matches   : 0

Entry        : 1020
time-range   : night                            Cur. Status    : Active
Log Id       : n/a
Src. IP      : 0.0.0.0/0                        Src. Port      : None
Dest. IP     : 10.10.1.1/16                     Dest. Port     : None
Protocol     : Undefined                        Dscp           : Undefined
ICMP Type    : Undefined                        ICMP Code      : Undefined
Fragment     : Off                              Option-present : Off
Sampling     : Off                              Int. Sampling  : On
IP-Option    : 0/0                              Multiple Option: Off
TCP-syn      : Off                              TCP-ack        : Off
Match action : Forward
Next Hop     : 172.22.184.101
Ing. Matches : 0                                Egr. Matches   : 0
===============================================================================
```

```
A:ALA-49#
```

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

Label	Description
Filter Id	The IP filter policy ID.
Scope	Template – The filter policy is of type Template.
	Exclusive – The filter policy is of type Exclusive.
Entries	The number of entries configured in this filter ID.
Applied	No – The filter policy ID has not been applied.
	Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward.
	Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Service Id	The service ID on which the filter policy ID is applied.
SAP	The Service Access Point on which the filter policy ID is applied.
(Ingress)	The filter policy ID is applied as an ingress filter policy on the interface.
(Egress)	The filter policy ID is applied as an egress filter policy on the interface.
Type	The type of service of the service ID.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete as no action was specified.
Log Id	The filter log ID.
Src. IP	The source IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
Dest. IP	The destination IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
Protocol	The protocol ID for the match criteria. Undefined indicates no protocol specified.
ICMP Type	The ICMP type match criterion. Undefined indicates no ICMP type specified.
Fragment	False – Configures a match on all non-fragmented IP packets.
	True – Configures a match on all fragmented IP packets.

Label	Description (Continued)
	Off – Fragments are not a matching criteria. All fragments and non-fragments implicitly match.
Sampling	Off – Specifies that traffic sampling is disabled. On – Specifies that traffic matching the associated IP filter entry is sampled.
IP-Option	Specifies matching packets with a specific IP option or a range of IP options in the IP header for IP filter match criteria.
TCP-syn	False – Configures a match on packets with the SYN flag set to false. True – Configured a match on packets with the SYN flag set to true. Off – The state of the TCP SYN flag is not considered as part of the match criteria.
Match action	Default – The filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete (no action was specified). Drop – Drop packets matching the filter entry. Forward – The explicit action to perform is forwarding of the packet. If the action is Forward, then if configured the nexthop information should be displayed, including Nexthop: <IP address>, Indirect: <IP address> or Interface: <IP interface name>.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Src. Port	The source TCP or UDP port number or port range.
Dest. Port	The destination TCP or UDP port number or port range.
Dscp	The DiffServ Code Point (DSCP) name.
ICMP Code	The ICMP code field in the ICMP header of an IP packet.
Option-present	Off – Specifies not to search for packets that contain the option field or have an option field of zero. On – Matches packets that contain the option field or have an option field of zero be used as IP filter match criteria.
Int. Sampling	Off – Interface traffic sampling is disabled. On – Interface traffic sampling is enabled.
Multiple Option	Off – The option fields are not checked. On – Packets containing one or more option fields in the IP header will be used as IP filter match criteria.

Label	Description (Continued)
TCP-ack	False – Configures a match on packets with the ACK flag set to false. True – configures a match on packets with the ACK flag set to true. Off – The state of the TCP ACK flag is not considered as part of the match criteria.h criteria.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

Sample Output

```
A:ALA-49# show filter ip 1 associations
===============================================================================
IP Filter
===============================================================================
Filter Id    : 1                                Applied        : Yes
Scope        : Template                         Def. Action    : Drop
Entries      : 1
-------------------------------------------------------------------------------
Filter Association : IP
-------------------------------------------------------------------------------
Service Id   : 1001                             Type           : VPLS
 - SAP    1/1/1:1001   (Ingress)
Service Id   : 2000                             Type           : IES
 - SAP    1/1/1:2000   (Ingress)
===============================================================================
Filter Match Criteria : IP
-------------------------------------------------------------------------------
Entry        : 10
Log Id       : n/a
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
Fragment     : Off                              Option-present : Off
Sampling     : Off                              Int. Sampling  : On
IP-Option    : 0/0                              Multiple Option: Off
TCP-syn      : Off                              TCP-ack        : Off
Match action : Drop
Ing. Matches : 0                                Egr. Matches   : 0
===============================================================================
A:ALA-49#
```

Output **Show Filter Associations (with TOD-suite specified) —** If a filter is referred to in a TOD Suite assignment, it is displayed in the show filter associations command output:

```
A:ALA-49# show filter ip 160 associations
===============================================================================
IP Filter
===============================================================================
Filter Id    : 160                              Applied        : No
Scope        : Template                         Def. Action    : Drop
```

```
Entries      : 0
-------------------------------------------------------------------------------
Filter Association : IP
-------------------------------------------------------------------------------
Tod-suite "english_suite"
 - ingress, time-range "day" (priority 5)
===============================================================================
A:ALA-49#
```

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

Label	Description
IP Filter Filter Id	The IP filter policy ID.
Scope	Template – The filter policy is of type Template. Exclusive – The filter policy is of type Exclusive.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward. Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	IP – Indicates the filter is an IP filter policy.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Egr. Matches	The number of egress filter matches/hits for the filter entry. Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.

Sample Output

```
*A:ALA-48# show filter ipv6 100 counters
===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 100                              Applied        : No
Scope        : Template                         Def. Action    : Forward
```

```
Entries      : 1
Description  : IPv6 filter configuration
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry        : 10
Ing. Matches : 9788619 pkts (978861900 bytes)
Egr. Matches : 9788619 pkts (978861900 bytes)
===============================================================================
*A:ALA-48#
```

ipv6

Syntax **ipv6**
ipv6 embedded [**inactive**]
ipv6 *ipv6-filter-id* **embedded** [**inactive**]
ipv6 *ipv6-filter-id* [**detail**]
ipv6 *ipv6-filter-id* **associations**
ipv6 *ipv6-filter-id* **type** *entry-type*
ipv6 *ipv6-filter-id* **counters** [**type** *entry-type*]
ipv6 *ipv6-filter-id* **entry** *entry-id* **counters**

Context show>filter

Description This command shows IPv6 filter information.

Parameters *ipv6-filter-id* — Displays detailed information for the specified IPv6 filter ID and filter entries.

Values 1 — 65535

entry *entry-id* **—** Displays information on the specified IPv6 filter entry ID for the specified filter ID.

Values 1 — 9999

associations — Appends information as to where the IPv6 filter policy ID is applied to the detailed filter policy ID output.

counters — Displays counter information for the specified IPv6 filter ID. Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.

embedded [**failed**] **—** Shows all embeddings, optionally shows failed embedding only, if *filter-id* is not specified shows all embedded filters.

type *entry-type* **—** specifies type of filter entry to display, values:

Values fixed, radius-insert, credit-control-insert, flowspec, embedded, radius-shared

Output **Show Filter (no filter-id specified) —** The following table describes the command output for the command when no filter ID is specified.

Label	Description
Filter Id	The IP filter ID
Scope	Template – The filter policy is of type template. Exclusive – The filter policy is of type exclusive.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Description	The IP filter policy description.
In	Shows embedding filter index
From	Shows embedded filters included
Priority	Shows priority of embedded filter
Inserted	Shows embedded/total number of entries from embedded filter Status: **OK**—embedding operation successful, if any entries are overwritten this will also be indicated. **Failed**—embedding failed, the reason is displayed (out of resources).
In	Shows embedding filter index

Sample Output

```
A:ALA-48# show filter ipv6
===============================================================================
IP Filters
===============================================================================
Filter-Id Scope      Applied Description
-------------------------------------------------------------------------------
100       Template   Yes     test
200       Exclusive  Yes
-------------------------------------------------------------------------------
Num IPv6 filters: 2
===============================================================================
A:ALA-48# show filter ipv6 embedded
================================================
IP Filter embedding
================================================
In        From    Priority   Inserted    Status
------------------------------------------------------------------------------
10        2        50        1/1         OK
          1        100       1/2         OK- 1 entry overwritten

20        2        100       0/5         Failed - out of resources
================================================
A:ALA-48#
```

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

Label	Description
Filter Id	The IP filter policy ID.
Scope	Template – The filter policy is of type template. Exclusive – The filter policy is of type exclusive.
Entries	The number of entries configured in this filter ID.
Description	The IP filter policy description.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward. Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	IP – Indicates the filter is an IP filter policy.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
Log Id	The filter log ID.
Src. IP	The source IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
Dest. IP	The destination IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
Protocol	The protocol ID for the match criteria. Undefined indicates no protocol specified.
ICMP Type	The ICMP type match criterion. Undefined indicates no ICMP type specified.
Fragment	False – Configures a match on all non-fragmented IP packets. True – Configures a match on all fragmented IP packets. Off – Fragments are not a matching criteria. All fragments and non-fragments implicitly match.

Label	Description (Continued)
Sampling	Off – Specifies that traffic sampling is disabled. On – Specifies that traffic matching the associated IP filter entry is sampled.
IP-Option	Specifies matching packets with a specific IP option or a range of IP options in the IP header for IP filter match criteria.
TCP-syn	False – Configures a match on packets with the SYN flag set to false. True – Configured a match on packets with the SYN flag set to true. Off – The state of the TCP SYN flag is not considered as part of the match criteria.
Match action	Default – The filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified. Drop – Drop packets matching the filter entry. Forward – The explicit action to perform is forwarding of the packet. If the action is Forward, then if configured the nexthop information should be displayed, including Nexthop: <IP address>, Indirect: <IP address> or Interface: <IP interface name>.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Src. Port	The source TCP or UDP port number or port range.
Dest. Port	The destination TCP or UDP port number or port range.
Dscp	The DiffServ Code Point (DSCP) name.
ICMP Code	The ICMP code field in the ICMP header of an IP packet.
Option-present	Off – Specifies not to search for packets that contain the option field or have an option field of zero. On – Matches packets that contain the option field or have an option field of zero be used as IP filter match criteria.
Int. Sampling	Off – Interface traffic sampling is disabled. On – Interface traffic sampling is enabled.
Multiple Option	Off – The option fields are not checked. On – Packets containing one or more option fields in the IP header will be used as IP filter match criteria.

Label	Description (Continued)
TCP-ack	False – Configures a match on packets with the ACK flag set to false. True – Configured a match on packets with the ACK flag set to true. Off – The state of the TCP ACK flag is not considered as part of the match criteria.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

Sample Output

```
A:ALA-48# show filter ipv6 100
===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 100                              Applied        : Yes
Scope        : Template                         Def. Action    : Forward
Entries      : 1
Description : test
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry        : 10
Log Id       : 101
Src. IP      : ::/0                             Src. Port      : None
Dest. IP     : ::/0                             Dest. Port     : None
Next Header  : Undefined                        Dscp           : Undefined
ICMP Type    : Undefined                        ICMP Code      : Undefined
TCP-syn      : Off                              TCP-ack        : Off
Match action : Drop
Ing. Matches : 0                                Egr. Matches   : 0
===============================================================================
A:ALA-48#
```

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

Label	Description
Filter Id	The IPv6 filter policy ID.
Scope	Template – The filter policy is of type Template. Exclusive – The filter policy is of type Exclusive.
Entries	The number of entries configured in this filter ID.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.

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.
Service Id	The service ID on which the filter policy ID is applied.
SAP	The Service Access Point on which the filter policy ID is applied.
(Ingress)	The filter policy ID is applied as an ingress filter policy on the interface.
(Egress)	The filter policy ID is applied as an egress filter policy on the interface.
Type	The type of service of the service ID.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete, no action was specified.
Log Id	The filter log ID.
Src. IP	The source IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
Dest. IP	The destination IP address and mask match criterion. 0.0.0.0/0 indicates no criterion specified for the filter entry.
Protocol	The protocol ID for the match criteria. Undefined indicates no protocol specified.
ICMP Type	The ICMP type match criterion. Undefined indicates no ICMP type specified.
Fragment	False – Configures a match on all non-fragmented IP packets. True – Configures a match on all fragmented IP packets. Off – Fragments are not a matching criteria. All fragments and non-fragments implicitly match.
Sampling	Off – Specifies that traffic sampling is disabled. On – Specifies that traffic matching the associated IP filter entry is sampled.
IP-Option	Specifies matching packets with a specific IP option or a range of IP options in the IP header for IP filter match criteria.
TCP-syn	False – Configures a match on packets with the SYN flag set to false. True – Configures a match on packets with the SYN flag set to true.

Label	Description (Continued)
	Off – The state of the TCP SYN flag is not considered as part of the match criteria.
Match action	Default – The filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete, no action was specified.
	Drop – Drop packets matching the filter entry.
	Forward – The explicit action to perform is forwarding of the packet. If the action is Forward, then if configured the nexthop information should be displayed, including Nexthop: <IP address>, Indirect: <IP address> or Interface: <IP interface name>.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Src. Port	The source TCP or UDP port number or port range.
Dest. Port	The destination TCP or UDP port number or port range.
Dscp	The DiffServ Code Point (DSCP) name.
ICMP Code	The ICMP code field in the ICMP header of an IP packet.
Option-present	Off – Specifies not to search for packets that contain the option field or have an option field of zero.
	On – Matches packets that contain the option field or have an option field of zero be used as IP filter match criteria.
Int. Sampling	Off – Interface traffic sampling is disabled.
	On – Interface traffic sampling is enabled.
Multiple Option	Off – The option fields are not checked.
	On – Packets containing one or more option fields in the IP header will be used as IP filter match criteria.
TCP-ack	False – Configures a match on packets with the ACK flag set to false.
	True – Configured a match on packets with the ACK flag set to true.
	Off – The state of the TCP ACK flag is not considered as part of the match criteria.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

Sample Output

```
A:ALA-48# show filter ipv6 1 associations
===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 1                                Applied        : Yes
Scope        : Template                         Def. Action    : Drop
Entries      : 1
-------------------------------------------------------------------------------
Filter Association : IPv6
-------------------------------------------------------------------------------
Service Id   : 2000                             Type           : IES
 - SAP    1/1/1:2000   (Ingress)
===============================================================================
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry        : 10
Log Id       : 101
Src. IP      : ::/0                             Src. Port      : None
Dest. IP     : ::/0                             Dest. Port     : None
Next Header  : Undefined                        Dscp           : Undefined
ICMP Type    : Undefined                        ICMP Code      : Undefined
TCP-syn      : Off                              TCP-ack        : Off
Match action : Drop
Ing. Matches : 0                                Egr. Matches   : 0
===============================================================================
A:ALA-48#
```

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

Label	Description
IP Filter Filter Id	The IP filter policy ID.
Scope	Template – The filter policy is of type template. Exclusive – The filter policy is of type exclusive.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward. Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	IP – Indicates the filter is an IP filter policy.

Label	Description (Continued)
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Egr. Matches	The number of egress filter matches/hits for the filter entry. Note that egress counters count the packets without Layer 2 encapsulation. Ingress counters count the packets with Layer 2 encapsulation.

Sample Output

```
A:ALA-48# show filter ipv6 8 counters
===============================================================================
IPv6 Filter
===============================================================================
Filter Id    : 8                                Applied        : Yes
Scope        : Template                         Def. Action    : Forward
Entries      : 4
Description  : Description for Ipv6 Filter Policy id # 8
-------------------------------------------------------------------------------
Filter Match Criteria : IPv6
-------------------------------------------------------------------------------
Entry        : 5
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

Entry        : 6
Ing. Matches : 0 pkts
Egr. Matches : 0 pkts

Entry        : 8
Ing. Matches : 160 pkts (14400 bytes)
Egr. Matches : 80 pkts (6880 bytes)

Entry        : 10
Ing. Matches : 80 pkts (7200 bytes)
Egr. Matches : 80 pkts (6880 bytes)

===============================================================================
A:ALA-48#
```

log

Syntax **log** *log-id* [**match** *string*] [**bindings**]

Context show>filter

Description This command shows the contents of a memory-based or a file-based filter log.

If the optional keyword **match** and *string* parameter are given, the command displays the given filter log from the first occurence of the given string.

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

Values 101 — 199

match *string* **—** Specifies to start displaying the filter log entries from the first occurence of *string*.

bindings — Displays the number of filter logs currently instantiated.

Output **Log Message Formatting —** Each filter log entry contains the following information in case summary log feature is not active (as appropriate).

Label	Description
yyyy/*mm*/*dd* *hh*:*mm*:*ss*	The date and timestamp for the log filter entry where *yyyy* is the year, *mm* is the month, *dd* is the day, *hh* is the hour, *mm* is the minute and *ss* is the second.
Filter	The filter ID and the entry ID which generated the filter log entry in the form *Filter_ID*:*Entry_ID*.
Desc	The description of the filter entry ID which generated the filter log entry.
Interface	The IP interface on which the filter ID and entry ID was associated which generated the filter log entry.
Action	The action of the filter entry on the logged packet.
Src MAC	The source MAC address of the logged packet.
Dst MAC	The destination MAC of the logged packet.
EtherType	The Ethernet type of the logged Ethernet type II packet.
Src IP	The source IP address of the logged packet. The source port will be displayed after the IP address as appropriate separated with a colon.
Dst IP	The destination IP address of the logged packet. The source port will be displayed after the IP address as appropriate separated with a colon.
Flags (IP flags)	M – The more fragments IP flag is set in the logged packet. DF – The do not fragment IP flag is set in the logged packet.
TOS	The TOS byte value in the logged packet.
Protocol	The IP protocol of the logged packet (TCP, UDP, ICMP or a protocol number in hex).

Label	Description (Continued)
Flags (TCP flags)	URG – Urgent bit set. ACK – Acknowledgement bit set. RST – Reset bit set. SYN – Synchronize bit set. FIN – Finish bit set.
HEX	If an IP protocol does not have a supported decode, the first 32 bytes following the IP header are printed in a hex dump. Log entries for non-IP packets include the Ethernet frame information and a hex dump of the first 40 bytes of the frame after the Ethernet header.
Total Log Instances (Allowed)	Specifies the maximum allowed instances of filter logs allowed on the system.
Total Log Instances (In Use)	Specifies the instances of filter logs presently existing on the system.
Total Log Bindings	Specifies the count of the filter log bindings presently existing on the system.
Type	The type of service of the service ID.
Filter ID	Uniquely identifies an IP filter as configured on the system.
Entry ID	The identifier which uniquely identifies an entry in a filter table.
Log	Specifies an entry in the filter log table.
Instantiated	Specifies if the filter log for this filter entry has or has not been instantiated.

If the packet being logged does not have a source or destination MAC address (i.e., POS) then the MAC information output line is omitted from the log entry.

In case log summary is active, the filter log mini-tables contain the following information..

Label	Description
Summary Log LogID	Displays the log ID.
Crit1	Summary criterion that is used as index into the mini-tables of the log.
TotCnt	The total count of logs.
ArpCnt	Displays the total number of ARP messages logged for this log ID.
Src... Dst...	The address type indication of the key in the mini-table.

Label	Description (Continued)
count	The number of messages logged with the specified source/destination address.
address	The address for which count messages where received.

Sample Filter Log Output

```
2007/04/13 16:23:09  Filter: 100:100  Desc: Entry-100
Interface: to-ser1  Action: Forward
Src MAC: 04-5b-01-01-00-02  Dst MAC: 04-5d-01-01-00-02  EtherType: 0800
Src IP: 10.10.0.1:646  Dst IP: 10.10.0.4:49509  Flags:   TOS: c0
Protocol: TCP  Flags: ACK

2007/04/13 16:23:10  Filter: 100:100  Desc: Entry-100
Interface: to-ser1  Action: Forward
Src MAC: 04-5b-01-01-00-02  Dst MAC: 04-5d-01-01-00-02  EtherType: 0800
Src IP: 10.10.0.1:646  Dst IP: 10.10.0.3:646  Flags:   TOS: c0
Protocol: UDP

2007/04/13 16:23:12  Filter: 100:100  Desc: Entry-100
Interface: to-ser1  Action: Forward
Src MAC: 04-5b-01-01-00-02  Dst MAC: 01-00-5e-00-00-05  EtherType: 0800
Src IP: 10.10.13.1  Dst IP: 224.0.0.5  Flags:   TOS: c0
Protocol: 89
Hex: 02 01 00 30 0a 0a 00 01 00 00 00 00 ba 90 00 00
     00 00 00 00 00 00 00 00 ff ff ff 00 00 03 02 01

A:ALA-A>config# show filter log bindings
===============================================================================
Filter Log Bindings
===============================================================================
Total Log Instances (Allowed)          : 2046
Total Log Instances (In Use)           : 0
Total Log Bindings                     : 0
-------------------------------------------------------------------------------
Type  FilterId EntryId   Log    Instantiated
-------------------------------------------------------------------------------
No Instances found
===============================================================================
A:ALA-A>config#
```

Note: A summary log will be printed only in case TotCnt is different from 0. Only the address types with at least 1 entry in the minitable will be printed.

```
A:ALA-A>config# show filter log 190
===============================================================================
Summary Log[190] Crit1: SrcAddr TotCnt:       723 ArpCnt:     83
 Mac          8  06-06-06-06-06-06
 Mac          8  06-06-06-06-06-05
 Mac          8  06-06-06-06-06-04
 Mac          8  06-06-06-06-06-03
 Mac          8  06-06-06-06-06-02
  Ip         16  6.6.6.1
  Ip         16  6.6.6.2
```

```
  Ip         16  6.6.6.3
  Ip         16  6.6.6.4
  Ip          8  6.6.6.5
Ipv6          8  3FE:1616:1616:1616:1616:1616::
Ipv6          8  3FE:1616:1616:1616:1616:1616:FFFF:FFFF
Ipv6          8  3FE:1616:1616:1616:1616:1616:FFFF:FFFE
Ipv6          8  3FE:1616:1616:1616:1616:1616:FFFF:FFFD
Ipv6          8  3FE:1616:1616:1616:1616:1616:FFFF:FFFC
===============================================================================
A:ALA-A
```

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.

Label	Description
Filter Id	The IP filter ID
Scope	Template – The filter policy is of type Template. Exclusiv – The filter policy is of type Exclusive.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Description	The MAC filter policy description.

Label	Description
MAC Filter Filter Id	The MAC filter policy ID.
Scope	Template – The filter policy is of type Template. Exclusiv – The filter policy is of type Exclusive.
Description	The IP filter policy description.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward. Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	MAC – Indicates the filter is an MAC filter policy.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
Description	The filter entry description.
FrameType	Ethernet – The entry ID match frame type is Ethernet IEEE 802.3. Ethernet II – The entry ID match frame type is Ethernet Type II.
Src MAC	The source MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion specified for the filter entry.
Dest MAC	The destination MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion specified for the filter entry.

Label	Description (Continued)
Dot1p	The IEEE 802.1p value for the match criteria. Undefined indicates no value is specified.
Ethertype	The Ethertype value match criterion.
DSAP	The DSAP value match criterion. Undefined indicates no value specified.
SSAP	SSAP value match criterion. Undefined indicates no value specified.
Snap-pid	The Ethernet SNAP PID value match criterion. Undefined indicates no value specified.
Esnap-oui-zero	Non-Zero – Filter entry matches a non-zero value for the Ethernet SNAP OUI. Zero – Filter entry matches a zero value for the Ethernet SNAP OUI. Undefined – No Ethernet SNAP OUI value specified.
Match action	Default – The filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete, no action was specified. Drop – Packets matching the filter entry criteria will be dropped. Forward – Packets matching the filter entry criteria is forwarded.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

Sample Detailed Output

```
===============================================================================
Mac Filter : 200
===============================================================================
Filter Id     : 200                           Applied       : No
Scope         : Exclusive                     D. Action     : Drop
Description : Forward SERVER sourced packets
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
-------------------------------------------------------------------------------
Entry         : 200                           FrameType     : 802.2SNAP
Description   : Not Available
Src Mac       : 00:00:5a:00:00:00 ff:ff:ff:00:00:00
Dest Mac      : 00:00:00:00:00:00 00:00:00:00:00:00
Dot1p         : Undefined                     Ethertype     : 802.2SNAP
DSAP          : Undefined                     SSAP          : Undefined
Snap-pid      : Undefined                     ESnap-oui-zero : Undefined
Match action  : Forward
Ing. Matches  : 0                             Egr. Matches  : 0
Entry         : 300 (Inactive)                FrameType     : Ethernet
Description   : Not Available
Src Mac       : 00:00:00:00:00:00 00:00:00:00:00:00
Dest Mac      : 00:00:00:00:00:00 00:00:00:00:00:00
Dot1p         : Undefined                     Ethertype     : Ethernet
```

```
DSAP          : Undefined                       SSAP          : Undefined
Snap-pid      : Undefined                       ESnap-oui-zero : Undefined
Match action  : Default
Ing. Matches  : 0                               Egr. Matches  : 0
===============================================================================
```

Filter Associations — The associations for a filter ID will be displayed if the **associations** keyword is specified. The assocation information is appended to the filter information. The following table describes the fields in the appended associations output.

Label	Description
Filter Association	Mac – The filter associations displayed are for a MAC filter policy ID.
Service Id	The service ID on which the filter policy ID is applied.
SAP	The Service Access Point on which the filter policy ID is applied.
Type	The type of service of the Service ID.
(Ingress)	The filter policy ID is applied as an ingress filter policy on the interface.
(Egress)	The filter policy ID is applied as an egress filter policy on the interface.

Sample Output

```
A:ALA-49# show filter mac 3 associations
===============================================================================
Mac Filter
===============================================================================
Filter ID : 3                               Applied       : Yes
Scope     : Template                        Def. Action   : Drop
Entries   : 1
-------------------------------------------------------------------------------
Filter Association : Mac
-------------------------------------------------------------------------------
Service Id: 1001                            Type          : VPLS
- SAP 1/1/1:1001   (Egress)
===============================================================================
A:ALA-49#
```

Filter Entry Counters Output — When the **counters** keyword is specified, the filter entry output displays the filter matches/hit information. The following table describes the command output for the command.

Sample Output

Label	Description
Mac Filter Filter Id	The MAC filter policy ID.
Scope	Template – The filter policy is of type Template. Exclusive – The filter policy is of type Exclusive.
Description	The MAC filter policy description.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward. Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	Mac – Indicates the filter is an MAC filter policy.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
FrameType	Ethernet – The entry ID match frame type is Ethernet IEEE 802.3. 802.2LLC – The entry ID match frame type is Ethernet IEEE 802.2 LLC. 802.2SNAP – The entry ID match frame type is Ethernet IEEE 802.2 SNAP. Ethernet II – The entry ID match frame type is Ethernet Type II.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

```
A:ALA-49# show filter mac 8 counters
===============================================================================
Mac Filter
===============================================================================
Filter Id   : 8                                 Applied         : Yes
Scope       : Template                          Def. Action     : Forward
Entries     : 2
Description : Description for Mac Filter Policy id # 8
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
-------------------------------------------------------------------------------
Entry       : 8                                 FrameType       : Ethernet
Ing. Matches: 80 pkts (5440 bytes)
```

```
Egr. Matches: 62 pkts (3968 bytes)

Entry       : 10                                FrameType       : Ethernet
Ing. Matches: 80 pkts (5440 bytes)
Egr. Matches: 80 pkts (5120 bytes)
```

li-mac

Syntax **li-mac** [*li-mac-filter-id* [**associations** | **counters**] [**entry** *entry-id*]]

Context show>filter

Description This command displays Lawful Intercept MAC filter information.

Parameters *li-mac-filter-id* — Displays detailed information for the specified Lawful Intercept filter ID and its filter entries.

Values 1— 65535

associations — Appends information as to where the Lawful Intercept filter policy ID is applied to the detailed filter policy ID output.

counters — Displays counter information for the specified Lawful Intercept filter ID.

entry *entry-id* — Displays information on the specified Lawful Intercept 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

Label	Description
`Filter Id`	The IP filter ID
`Scope`	`Template` – The filter policy is of type Template.
	`Exclusiv` – The filter policy is of type Exclusive.
`Applied`	`No` – The filter policy ID has not been applied.
	`Yes` – The filter policy ID is applied.
`Description`	The MAC filter policy description.

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

Label	Description
`MAC Filter Filter Id`	The MAC filter policy ID.

Label	Description (Continued)
Scope	Template – The filter policy is of type Template. Exclusiv – The filter policy is of type Exclusive.
Description	The IP filter policy description.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward. Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	MAC – Indicates the filter is an MAC filter policy.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
Description	The filter entry description.
FrameType	Ethernet – The entry ID match frame type is Ethernet IEEE 802.3. Ethernet II – The entry ID match frame type is Ethernet Type II.
Src MAC	The source MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion specified for the filter entry.
Dest MAC	The destination MAC address and mask match criterion. When both the MAC address and mask are all zeroes, no criterion specified for the filter entry.
Dot1p	The IEEE 802.1p value for the match criteria. Undefined indicates no value is specified.
Ethertype	The Ethertype value match criterion.
DSAP	The DSAP value match criterion. Undefined indicates no value specified.
SSAP	SSAP value match criterion. Undefined indicates no value specified.
Snap-pid	The Ethernet SNAP PID value match criterion. Undefined indicates no value specified.
Esnap-oui-zero	Non-Zero – Filter entry matches a non-zero value for the Ethernet SNAP OUI. Zero – Filter entry matches a zero value for the Ethernet SNAP OUI. Undefined – No Ethernet SNAP OUI value specified.

Label	Description (Continued)
Match action	Default – The filter does not have an explicit forward or drop match action specified. If the filter entry ID indicates the entry is Inactive, the filter entry is incomplete, no action was specified. Drop – Packets matching the filter entry criteria will be dropped. Forward – Packets matching the filter entry criteria is forwarded.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

Sample Detailed Output

```
# show li filter li-mac "testLiMacFilter"

===============================================================================
LI Mac Filter
===============================================================================
Filter Id   : testLiMacFilter                 Associated      : Yes
Entries     : 4
Description : test LI Mac filter setup
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
-------------------------------------------------------------------------------
Entry       : 10                              FrameType       : Ethernet
Description : entry 10
Src Mac     : 01:02:03:04:05:06 ff:ff:ff:ff:ff:ff
Dest Mac    :
LI Source   : Yes
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

Entry       : 20                              FrameType       : Ethernet
Description : entry 20
Src Mac     :
Dest Mac    : 01:02:03:04:05:06 ff:ff:ff:ff:ff:ff
LI Source   : Yes
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

Entry       : 30                              FrameType       : Ethernet
Description : test 30
Src Mac     :
Dest Mac    :
LI Source   : Yes
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

Entry       : 50                              FrameType       : Ethernet
Description : entry 50
Src Mac     : 00:00:01:66:00:00 00:00:0f:ff:00:00
Dest Mac    :
LI Source   : No
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts
```

Filter Associations — The associations for a filter ID will be displayed if the **associations** keyword is specified. The assocation information is appended to the filter information. The following table describes the fields in the appended associations output.

Label	Description
Filter Association	Mac – The filter associations displayed are for a MAC filter policy ID.
Service Id	The service ID on which the filter policy ID is applied.
SAP	The Service Access Point on which the filter policy ID is applied.
Type	The type of service of the Service ID.
(Ingress)	The filter policy ID is applied as an ingress filter policy on the interface.
(Egress)	The filter policy ID is applied as an egress filter policy on the interface.

Sample Output

```
# show li filter li-mac "testLiMacFilter" association

===============================================================================
LI Mac Filter
===============================================================================
Filter Id   : testLiMacFilter                 Associated      : Yes
Entries     : 4
Description : test LI Mac filter setup
-------------------------------------------------------------------------------
Filter Association : Mac
-------------------------------------------------------------------------------
mac filter 1
  Service Id  : 60                            Type            : VPLS
    - SAP    1/1/6:7  (Ingress)
    - SAP    1/1/6:9  (Egress)
```

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

Label	Description
Mac Filter Filter Id	The MAC filter policy ID.
Scope	Template – The filter policy is of type Template. Exclusive – The filter policy is of type Exclusive.
Description	The MAC filter policy description.
Applied	No – The filter policy ID has not been applied. Yes – The filter policy ID is applied.
Def. Action	Forward – The default action for the filter ID for packets that do not match the filter entries is to forward. Drop – The default action for the filter ID for packets that do not match the filter entries is to drop.
Filter Match Criteria	Mac – Indicates the filter is an MAC filter policy.
Entry	The filter ID filter entry ID. If the filter entry ID indicates the entry is (Inactive), then the filter entry is incomplete as no action has been specified.
FrameType	Ethernet – The entry ID match frame type is Ethernet IEEE 802.3. 802.2LLC – The entry ID match frame type is Ethernet IEEE 802.2 LLC. 802.2SNAP – The entry ID match frame type is Ethernet IEEE 802.2 SNAP. Ethernet II – The entry ID match frame type is Ethernet Type II.
Ing. Matches	The number of ingress filter matches/hits for the filter entry.
Egr. Matches	The number of egress filter matches/hits for the filter entry.

```
# show li filter li-mac "testLiMacFilter" counters

===============================================================================
LI Mac Filter
===============================================================================
Filter Id   : testLiMacFilter                 Associated      : Yes
Entries     : 4
Description : test LI Mac filter setup
-------------------------------------------------------------------------------
Filter Match Criteria : Mac
-------------------------------------------------------------------------------
Entry       : 10
Description : entry 10
```

```
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

Entry       : 20
Description : entry 20
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

Entry       : 30
Description : test 30
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts

Entry       : 50
Description : entry 50
Ing. Matches: 0 pkts
Egr. Matches: 0 pkts
```

redirect-policy

Syntax **redirect-policy** {*redirect-policy-name* [**dest** *ip-address*] [**association**]}

Context show>filter

Description This command shows redirect filter information.

Parameters *redirect-policy-name* — Displays information for the specified redirect policy.

dest *ip-address* **—** Directs the router to use a specified IP address for communication.

association — Appends association information.

Output **Redirect Policy Output —** The following table describes the fields in the redirect policy command output.

Label	Description
Redirect Policy	Specifies a specific redirect policy.
Applied	Specifies whether the redirect policy is applied to a filter policy entry.
Description	Displays the user-provided description for this redirect policy.
Active Destination	ip address – Specifies the IP address of the active destination. none – Indicates that there is currently no active destination.
Destination	Specifies the destination IP address.
Oper Priority	Specifies the operational value of the priority for this destination. The highest operational priority across multiple destinations is used as the preferred destination.
Admin Priority	Specifies the configured base priority for the destination.

Label	Description (Continued)
Admin State	Specifies the configured state of the destination. Out of Service – Tests for this destination will not be conducted.
Oper State	Specifies the operational state of the destination.
Ping Test	Specifies the name of the ping test.
Timeout	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.
Interval	Specifies the amount of time in seconds between consecutive requests sent to the far end host.
Drop Count	Specifies the number of consecutive requests that must fail for the destination to declared unreachable.
Hold Down	Specifies the amount of time in seconds that the system should be held down if any of the test has marked it unreachable.
Hold Remain	Specifies the amount of time in seconds that the system will remain in a hold down state before being used again.
Last Action at	Displays a time stamp of when this test received a response for a probe that was sent out.
SNMP Test	Specifies the name of the SNMP test.
URL Test	Specifies the name of the URL test.

Sample Output

```
A:ALA-A>config>filter# show filter redirect-policy
===============================================================================
Redirect Policies
===============================================================================
Redirect Policy                 Applied Description
-------------------------------------------------------------------------------
wccp                            Yes
redirect1                       Yes     New redirect info
redirect2                       Yes     Test test test test
===============================================================================
ALA-A>config>filter#


ALA-A>config>filter# show filter redirect-policy redirect1
===============================================================================
Redirect Policy
===============================================================================
Redirect Policy: redirect1                      Applied      : Yes
Description    : New redirect info
Active Dest    : 10.10.10.104
-------------------------------------------------------------------------------
```

```
Destination    : 10.10.10.104
-------------------------------------------------------------------------------
Description    : SNMP_to_104
Admin Priority : 105                              Oper Priority: 105
Admin State    : Up                               Oper State   : Up

SNMP Test      : SNMP-1
Interval       : 30                               Timeout      : 1
Drop Count     : 30
Hold Down      : 120                              Hold Remain  : 0
Last Action at : None Taken
-------------------------------------------------------------------------------
Destination    : 10.10.10.105
-------------------------------------------------------------------------------
Description    : another test
Admin Priority : 95                               Oper Priority: 105
Admin State    : Up                               Oper State   : Down

Ping Test
Interval       : 1                                Timeout      : 30
Drop Count     : 5
Hold Down      : 0                                Hold Remain  : 0
Last Action at : 03/19/2007 00:46:55              Action Taken : Disable
-------------------------------------------------------------------------------
Destination    : 10.10.10.106
-------------------------------------------------------------------------------
Description    : (Not Specified)
Admin Priority : 90                               Oper Priority: 90
Admin State    : Up                               Oper State   : Down

URL Test       : URL_to_Proxy
Interval       : 10                               Timeout      : 10
Drop Count     : 3
Hold Down      : 0                                Hold Remain  : 0
Last Action at : 03/19/2007 05:04:15              Action Taken : Disable
Priority Change: 0                                Return Code  : 0
===============================================================================
A:ALA-A>config>filter#


A:ALA-A>show filter redirect-policy redirect1 dest 10.10.10.106
===============================================================================
Redirect Policy
===============================================================================
Redirect Policy: redirect1                        Applied      : Yes
Description    : New redirect info
Active Dest    : 10.10.10.104
-------------------------------------------------------------------------------
Destination    : 10.10.10.106
-------------------------------------------------------------------------------
Description    : (Not Specified)
Admin Priority : 90                               Oper Priority: 90
Admin State    : Up                               Oper State   : Down

URL Test       : URL_to_Proxy
Interval       : 10                               Timeout      : 10
Drop Count     : 3
Hold Down      : 0                                Hold Remain  : 0
Last Action at : 03/19/2007 05:04:15              Action Taken : Disable
```

```
Priority Change: 0                                  Return Code  : 0
===============================================================================
ALA-A#
```

match-list

Syntax **match-list**

Context show>filter

Description This command displays information for match lists used in filter policies (IOM and CPM).

ip-prefix-list

Syntax **ip-prefix-list** [*prefix-list-name*]
ip-prefix-list *prefix-list-name* **references**

Context show>filter>match-list

Description This command displays IPv4 prefixes information for match criteria in IPv4 ACL and CPM filter policies.

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.

ipv6-prefix-list

Syntax **ipv6-prefix-list** [*prefix-list-name*]
ipv6-prefix-list *prefix-list-name* **references**

Context show>filter>match-list

Description This command displays IPv6 prefixes information for match criteria in IPv6 ACL and CPM filter policies.

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.

port-list

Syntax **port-list** [*port-list-name*]
port-list p*ort-list-name* **references**

Context show>filter>match-list

Description This command displays TCP/UDP port values or ranges for match criteria in IPv4 and IPv6 ACL and CPM 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.

Clear Commands

ip

Syntax **ip** *ip-filter-id* [**entry** *entry-id*] [**ingress** | **egress**]

Context clear>filter

Description Clears the counters associated with the IP filter policy.

By default, all counters associated with the filter policy entries are reset. The scope of which counters are cleared can be narrowed using the command line parameters.

Default clears all counters associated with the IP filter policy entries.

Parameters *ip-filter-id* — The IP filter policy ID.

Values 1 — 65535

entry-id — Specifies that only the counters associated with the specified filter policy entry will be cleared.

Values 1 — 65535

ingress — Specifies to only clear the ingress counters.

egress — Specifies to only clear the egress counters.

ipv6

Syntax **ipv6** *ip-filter-id* [**entry** *entry-id*] [**ingress** | **egress**]

Context clear>filter

Description Clears the counters associated with the IPv6 filter policy.

By default, all counters associated with the filter policy entries are reset. The scope of which counters are cleared can be narrowed using the command line parameters.

Default Clears all counters associated with the IPv6 filter policy entries.

Parameters *ip-filter-id* — The IP filter policy ID.

Values 1 — 65535

entry-id — Specifies that only the counters associated with the specified filter policy entry will be cleared.

Values 1 — 65535

ingress — Specifies to only clear the ingress counters.

egress — Specifies to only clear the egress counters.

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

filter

Syntax **filter ip** *ip-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor

Description This command monitors the counters associated with the IP filter policy.

Parameters *ip-filter-id* — The IP filter policy ID.

Values 1 — 65535

entry-id — Specifies that only the counters associated with the specified filter policy entry will be monitored.

Values 1 — 65535

interval — Configures the interval for each display in seconds.

Default 10 seconds

Values 3 — 60

repeat *repeat* — Configures how many times the command is repeated.

Default 10

Values 1 — 999

absolute — When the **absolute** keyword is specified, the raw statistics are displayed, without processing. No calculations are performed on the delta or rate statistics.

rate — When the **rate** keyword is specified, the rate-per-second for each statistic is displayed instead of the delta.

filter

Syntax **filter ipv6** *ipv6-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor

Description This command monitors the counters associated with the IPv6 filter policy.

Parameters *ipv6-filter-id* — The IP filter policy ID.

Values 1 — 65535

entry-id — Specifies that only the counters associated with the specified filter policy entry will be moniitored.

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.

filter

Syntax **filter mac** *mac-filter-id* **entry** *entry-id* [**interval** *seconds*] [**repeat** *repeat*] [**absolute** | **rate**]

Context monitor

Description This command monitors the counters associated with the MAC filter policy.

Parameters *mac-filter-id* — The MAC filter policy ID.

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.