Access List Commands

This module describes the Cisco IOS XR software commands used to configure IP Version 4 (IPv4) and IP Version 6 (IPv6) access lists.

For detailed information about ACL concepts, configuration tasks, and examples, refer to the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

atomic-disable

Allows all traffic that matches the ACL rule, or denies all traffic on the interface, while the ACL is being modified.

hardware access-list atomic-disable [**default-action permit**]

Syntax Description

default-action permit	Allows all traffic on the interface that matches the ACL rule, while the ACL is being modified.
<none>	Denies all traffic on the interface while the ACL is being modified.

Command Default

None

Command Modes

Privileged Executive mode

Command History

Release	Modification
Release 6.2.1	This command was introduced.

Usage Guidelines

When atomic ACL updates are disabled, the ACL is detached, and the ACL rules are not applied during the ACE modification process. Hence, it is recommended to configure to either permit or deny all traffic until the modification is complete.

For more information, see the Atomic ACL Updates By Using the Disable Option section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5000 Series Routers*.

Example

To disable atomic updates on the hardware, by permitting packets that match the ACE rule, use the following configuration.

```
RP/0/RP0/CPU0:router# hardware access-list atomic-disable default-action permit
```

To disable atomic updates on the hardware, by denying all packets until the modification is complete, use the following configuration.

```
RP/0/RP0/CPU0:router# hardware access-list atomic-disable
```

clear access-list ipv4

To clear IPv4 access list counters, use the **clear access-list ipv4** command in XR EXEC mode.

clear access-list ipv4 *access-list name* [{*sequence-number*| **ingress**}] [{**location** *node-id*|**sequence** *number*}]

Syntax Description

access-list-name	Name of a particular IPv4 access list. The name cannot contain a spaces or quotation marks, but can include numbers.
sequence-number	(Optional) Specific sequence number with which counters are cleared for an access list. Range is 1 to 2147483644.
ingress	Specifies an inbound direction.
type	Interface type. For more information, use the question mark (?) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.
location *node-id*	(Optional) Clears hardware resource counters from the designated node. The *node-id* argument is entered in the *rack/slot/module* notation.
sequence *number*	(Optional) Clears counters for an access list with a specific sequence number. Range is 1 to 2147483644.

Command Default

The default clears the specified IPv4 access list.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **clear access-list ipv4** command to clear counters for a specified configured access list. Use a sequence number to clear counters for an access list with a specific sequence number.

Use an asterisk (***)** in place of the *access-list-name* argument to clear all access lists.

Task ID

Task ID	Operations
basic-services	read, write
acl	read, write

Task ID	Operations
bgp	read, write, execute

Examples

In the following example, counters for an access list named *marketing* are cleared:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  10 permit ip 192.168.34.0 0.0.0.255
  20 permit ip 172.16.0.0 0.0.255.255
  30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30

RP/0/RP0/CPU0:router# clear access-list ipv4 marketing

RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  10 permit ip 192.168.34.0 0.0.0.255 any
  20 permit ip 172.16.0.0 0.0.255.255 any
  30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30
```

copy access-list ipv4

To create a copy of an existing IPv4 access list, use the **copy access-list ipv4** command in XR EXEC mode.

copy access-list ipv4 *source-acl destination-acl*

Syntax Description

source-acl	Name of the access list to be copied.
destination-acl	Name of the destination access list where the contents of the *source-acl* argument is copied.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **copy access-list ipv4** command to copy a configured access list. Use the *source-acl* argument to specify the access list to be copied and the *destination-acl* argument to specify where to copy the contents of the source access list. The *destination-acl* argument must be a unique name; if the *destination-acl* argument name exists for an access list or prefix list, the access list is not copied. The **copy access-list ipv4** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists or prefix lists.

Task ID

Task ID	Operations
acl	read, write
filesystem	execute

Examples

In the following example, a copy of access list list-1 is created:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 list-1

ipv4 access-list list-1
  10 permit tcp any any log
  20 permit ip any any
RP/0/RP0/CPU0:router# copy access-list ipv4 list-1 list-2
RP/0/RP0/CPU0:router# show access-lists ipv4 list-2
ipv4 access-list list-2
  10 permit tcp any any log
  20 permit ip any any
```

In the following example, copying the access list list-1 to list-3 is denied because a list-3 access list already exists:

```
RP/0/RP0/CPU0:router# copy access-list ipv4 list-1 list-3

list-3 exists in access-list

RP/0/RP0/CPU0:router# show access-lists ipv4 list-3

ipv4 access-list list-3
  10 permit ip any any
  20 deny tcp any any log
```

deny (IPv4)

To set conditions for an IPv4 access list, use the **deny** command in access list configuration mode. There are two versions of the **deny** command: **deny** (source), and **deny** (protocol). To remove a condition from an access list, use the **no** form of this command.

[*sequence-number*] **deny** *source* [*source-wildcard*] **counter** *counter-name* [{**log**}]

[*sequence-number*] **deny***protocol source source-wildcard destination destination-wildcard* [**precedence***precedence*] [**dscp***dscp*] [**fragments**] [*packet-length operator packet-length value*] [**log**] [**ttl** *ttl value* [*value1....value2*]] [**counter** *counter-name*]

no *sequence-number*

Internet Control Message Protocol (ICMP)

[*sequence-number*] **deny** **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type*] [*icmp-code*] [**precedence** *precedence*] [**dscp** *dscp*] **[fragments]** [{**log**}] [**counter** *counter-name*] **[icmp-off]**

Internet Group Management Protocol (IGMP)

[*sequence-number*] **deny** **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] **[fragments]** [{**log**}] [**counter** *counter-name*]

User Datagram Protocol (UDP)

[*sequence-number*] **deny** **udp** *source source-wildcard* [*operator* {*portprotocol-port*}] *destination destination-wildcard* [*operator* {*portprotocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] **[fragments]** [{**log**}] [**counter** *counter-name*]

Syntax Description

sequence-number	(Optional) Number of the **deny** statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

protocol	Name or number of an IP protocol. It can be one of the keywords , **esp** , **gre** , **icmp** , **igmp** , **igrp** , **ip** , **ipinip** , **nos** , **ospf** , **pim** , **pcp** , **tcp** , or **udp** , or an integer from 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. ICMP, and TCP allow further qualifiers, which are described later in this table.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level (as specified by a number from 0 to 7) or by the following names: • **routine** —Match packets with routine precedence (0) • **priority** —Match packets with priority precedence (1) • **immediate** —Match packets with immediate precedence (2) • **flash** —Match packets with flash precedence (3) • **flash-override** —Match packets with flash override precedence (4) • **critical** —Match packets with critical precedence (5) • **internet** —Match packets with internetwork control precedence (6) • **network** —Match packets with network control precedence (7)

dscp *dscp*	(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows: • **0**–**63**–Differentiated services codepoint value • **af11**—Match packets with AF11 dscp (001010) • **af12**—Match packets with AF12 dscp (001100) • **af13**—Match packets with AF13 dscp (001110) • **af21**—Match packets with AF21 dscp (010010) • **af22**—Match packets with AF22 dscp (010100) • **af23**—Match packets with AF23 dscp (010110) • **af31**—Match packets with AF31 dscp (011010) • **af32**—Match packets with AF32 dscp (011100) • **af33**—Match packets with AF33 dscp (011110) • **af41**—Match packets with AF41 dscp (100010) • **af42**—Match packets with AF42 dscp (100100) • **af43**—Match packets with AF43 dscp (100110) • **cs1**—Match packets with CS1 (precedence 1) dscp (001000) • **cs2**—Match packets with CS2 (precedence 2) dscp (010000) • **cs3**—Match packets with CS3 (precedence 3) dscp (011000) • **cs4**—Match packets with CS4 (precedence 4) dscp (100000) • **cs5**—Match packets with CS5 (precedence 5) dscp (101000) • **cs6**—Match packets with CS6 (precedence 6) dscp (110000) • **cs7**—Match packets with CS7 (precedence 7) dscp (111000) • **default**—Default DSCP (000000) • **ef**—Match packets with EF dscp (101110)
fragments	(Optional) Causes the software to examine fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches a flow, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
ttl value [*value1*. . *value2*[	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
icmp-off	(Optional) Turns off ICMP generation for denied packets.
icmp-type	(Optional) ICMP message type for filtering ICMP packets. Range is from 0 to 255.

icmp-code	(Optional) ICMP message code for filtering ICMP packets. Range is from 0 to 255.
igmp-type	(Optional) IGMP message type (0 to 15) or message name for filtering IGMP packets, as follows: • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • trace • v2-leave • v2-report • v3-report
operator	(Optional) Operator is used to compare source or destination ports. Possible operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard* values, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard* values, it must match the destination port. If the operator is positioned after the **ttl** keyword, it matches the TTL value. The **range** operator requires two port numbers. All other operators require one port number.
port	Decimal number of a TCP or UDP port. A port number is a number from 0 to 65535. TCP ports can be used only when filtering TCP. UDP ports can be used only when filtering UDP.
protocol-port	Name of a TCP or UDP port. TCP and UDP port names are listed in the "Usage Guidelines" section. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | **-**	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with + or **-** . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Optional) For the TCP protocol **match-any** , **match-all** . Flag names are: **ack** , **fin** , **psh** , **rst** , **syn** , **urg**.

counter	(Optional) Enables accessing ACL counters using SNMP query.
counter-name	Defines an ACL counter name.

Command Default

There is no specific condition under which a packet is denied passing the IPv4 access list.

ICMP message generation is enabled by default.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **deny** command following the **ipv4 access-list** command to specify conditions under which a packet cannot pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, or **remark** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

The following is a list of precedence names:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The following is a list of ICMP message type names:

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable

- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- ttl-exceeded
- unreachable

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data

- gopher
- hostname
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

The following UDP port names can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs

- talk
- tftp
- time
- who
- xdmcp

Use the following flags in conjunction with the **match-any** and **match-all** keywords and the + and - signs to select the flags to display:

- ack
- fin
- psh
- rst
- syn

For example, **match-all** + *ack* + *syn* displays TCP packets with both the ack *and* syn flags set, or **match-any** + *ack* - *syn* displays the TCP packets with the ack set *or* the syn not set.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

This example shows how to set a deny condition for an access list named Internet filter:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 deny 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203
 range 1300 1400
RP/0/RP0/CPU0:router(config-ipv4-acl)# permit 10.0.0.0 0.255.255.255
```

ipv4 access-group

To control access to an interface, use the **ipv4 access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

ipv4 access-group *access-list-name* {**ingress**}
no ipv4 access-group *access-list-name* {**ingress**}

Syntax Description

access-list-name	Name of an IPv4 access list as specified by an **ipv4 access-list** command.
ingress	Filters on inbound packets.

Command Default

The interface does not have an IPv4 access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **ipv4 access-group** command to control access to an interface. To remove the specified access group, use the **no** form of the command. Use the *access-list-name* argument to specify a particular IPv4 access list. Use the **ingress** keyword to filter on inbound packets. Use the *hardware-count* argument to enable hardware counters for the access group.

Filtering of MPLS packets through interface ACL is not supported.

If the access list permits the addresses, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

If the specified access list does not exist, all packets are passed.

Task ID

Task ID	Operations
acl	read, write
network	read, write

Examples

The following example shows how to apply filters on packets from tenGigE interface 0/0/0/2:

```
RP/0/RP0/CPU0:router(config)# interface tenGigE 0/0/0/2
RP/0/RP0/CPU0:router(config-if)# ipv4 access-group p-ingress-filter ingress
```

ipv4 access-list

To define an IPv4 access list by name, use the **ipv4 access-list** command in XR Config mode. To remove all entries in an IPv4 access list, use the **no** form of this command.

ipv4 access-list *name*
no ipv4 access-list *name*

Syntax Description

name	Name of the access list. Names cannot contain a space or quotation marks.

Command Default

No IPv4 access list is defined.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **ipv4 access-list** command to configure an IPv4 access list. This command places the router in access list configuration mode, in which the denied or permitted access conditions must be defined with the **deny** or **permit** command.

Use the **ipv4 access-group** command to apply the access list to an interface.

Task ID

Task ID	Operations
acl	read, write

Examples

This example shows how to define a standard access list named Internetfilter:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit 10.0.0.0 0.255.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 39 remark Block BGP traffic from 172.16 net.
RP/0/RP0/CPU0:router(config-ipv4-acl)# 40 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203
 range 1300 1400
```

ipv4 access-list log-update rate

To specify the rate at which IPv4 access lists are logged, use the **ipv4 access-list log-update rate** command in XR Config mode. To return the update rate to the default setting, use the **no** form of this command.

ipv4 access-list log-update rate *rate-number*
no ipv4 access-list log-update rate *rate-number*

Syntax Description

rate-number	Rate at which IPv4 access hit logs are generated per second on the router. Range is 1 to 1000.

Command Default

Default is 1.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

The *rate-number* argument applies to all the IPv4 access-lists configured on the interfaces. That is, at any given time there can be between 1 and 1000 log entries for the system.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

The following example shows how to configure a IPv4 access hit logging rate for the system:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list log-update rate 10
```

ipv4 access-list log-update threshold

To specify the number of updates that are logged for IPv4 access lists, use the **ipv4 access-list log-update threshold** command in XR Config mode. To return the number of logged updates to the default setting, use the **no** form of this command.

ipv4 access-list log-update threshold *update-number*
no ipv4 access-list log-update threshold *update-number*

Syntax Description

update-number	Number of updates that are logged for every IPv4 access list configured on the router. Range is 0 to 2147483647.

Command Default

For IPv4 access lists, 2147483647 updates are logged.

Command Modes

XR Config mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

IPv4 access list updates are logged at 5-minute intervals, following the first logged update. Configuring a lower number of updates (a number lower than the default) is useful when more frequent update logging is desired.

Task ID

Task ID	Operations
basic-services	read, write
acl	read, write

Examples

This example shows how to configure a log threshold of ten updates for every IPv4 access list configured on the router:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list log-update threshold 10
```

permit (IPv4)

To set conditions for an IPv4 access list, use the **permit** command in access list configuration mode. There are two versions of the **permit** command: **permit** (source), and **permit** (protocol). To remove a condition from an access list, use the **no** form of this command.

[*sequence-number*] **permit** *source* [*source-wildcard*] [{**log**}]
[*sequence-number*] **permit** *protocol* *net-group* *source-net-object-group-name* *destination* *source-port-object-group-name* **net-group** *destination-net-object-group-name* **port-group** *destination-port-object-group-name* [**capture**][**precedence** *precedence*]] [**dscp** *dscp*] **[fragments]** [{**log**}] [**ttl** *ttl value* [*value1* **. . .** *value2*]][**counter** *counter-name*]
no *sequence-number*

Internet Control Message Protocol (ICMP)
[*sequence-number*] **permit icmp** *source source-wildcard destination destination-wildcard* [*icmp-type*] [*icmp-code*] [**precedence** *precedence*] [**dscp** *dscp*] **[fragments]** [**counter** *counter-name*]

Internet Group Management Protocol (IGMP)
[*sequence-number*] **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**dscp** *value*] **[fragments]** [**counter** *counter-name*]

User Datagram Protocol (UDP)
[*sequence-number*] **permit udp** *source source-wildcard* [*operator* {*portprotocol-port*}] *destination destination-wildcard* [*operator* {*portprotocol-port*}] [**precedence** *precedence*] [**dscp** *dscp*] **[fragments]** [**counter** *counter-name*]

Syntax Description

sequence-number	(Optional) Number of the **permit** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483644. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *source* combination as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
protocol	Name or number of an IP protocol. It can be one of the keywords , **esp** , , **icmp** , **igmp** , **igrp** , **ip** , **ipinip** , **nos** , **ospf** , **pim** , **pcp** , **tcp** , or **udp** , or an integer from 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip** keyword. ICMP, and TCP allow further qualifiers, which are described later in this table.

destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use the **host** *destination* combination as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

precedence *precedence*	(Optional) Packets can be filtered by precedence level (as specified by a number from 0 to 7) or by the following names: • **Routine** —Match packets with routine precedence (0) • **priority** —Match packets with priority precedence (1) • **immediate** —Match packets with immediate precedence (2) • **flash** —Match packets with flash precedence (3) • **flash-override** —Match packets with flash override precedence (4) • **critical** —Match packets with critical precedence (5) • **internet** —Match packets with internetwork control precedence (6) • **network** —Match packets with network control precedence (7)
capture	Captures matching traffic. When the acl command is configured on the source mirroring port, if the ACL configuration command does not use the **capture** keyword, no traffic gets mirrored. If the ACL configuration uses the **capture** keyword, but the acl command is not configured on the source port, then the whole port traffic is mirrored and the **capture** action does not have any affect.

dscp *dscp*	(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows: • 0–63—Differentiated services codepoint value • af11—Match packets with AF11 dscp (001010) • af12—Match packets with AF12 dscp (001100) • af13—Match packets with AF13 dscp (001110) • af21—Match packets with AF21 dscp (010010) • af22—Match packets with AF22 dscp (010100) • af23—Match packets with AF23 dscp (010110) • af31—Match packets with AF31 dscp (011010) • af32—Match packets with AF32 dscp (011100) • af33—Match packets with AF33 dscp (011110) • af41—Match packets with AF41 dscp (100010) • af42—Match packets with AF42 dscp (100100) • af43–Match packets with AF43 dscp (100110) • cs1—Match packets with CS1 (precedence 1) dscp (001000) • cs2—Match packets with CS2 (precedence 2) dscp (010000) • cs3—Match packets with CS3 (precedence 3) dscp (011000) • cs4—Match packets with CS4 (precedence 4) dscp (100000) • cs5—Match packets with CS5 (precedence 5) dscp (101000) • cs6—Match packets with CS6 (precedence 6) dscp (110000) • cs7—Match packets with CS7 (precedence 7) dscp (111000) • default—Default DSCP (000000) • ef—Match packets with EF dscp (101110)

dscp range *dscp dscp*	(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for *dscp* are as follows: • 0–63—Differentiated services codepoint value • af11—Match packets with AF11 dscp (001010) • af12—Match packets with AF12 dscp (001100) • af13—Match packets with AF13 dscp (001110) • af21—Match packets with AF21 dscp (010010) • af22—Match packets with AF22 dscp (010100) • af23—Match packets with AF23 dscp (010110) • af31—Match packets with AF31 dscp (011010) • af32—Match packets with AF32 dscp (011100) • af33—Match packets with AF33 dscp (011110) • af41—Match packets with AF41 dscp (100010) • af42—Match packets with AF42 dscp (100100) • af43–Match packets with AF43 dscp (100110) • cs1—Match packets with CS1 (precedence 1) dscp (001000) • cs2—Match packets with CS2 (precedence 2) dscp (010000) • cs3—Match packets with CS3 (precedence 3) dscp (011000) • cs4—Match packets with CS4 (precedence 4) dscp (100000) • cs5—Match packets with CS5 (precedence 5) dscp (101000) • cs6—Match packets with CS6 (precedence 6) dscp (110000) • cs7—Match packets with CS7 (precedence 7) dscp (111000) • default—Default DSCP (000000) • ef—Match packets with EF dscp (101110)

fragments	(Optional) Causes the software to examine noninitial fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches a flow, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.
ttl	(Optional) Turns on matching against time-to-life (TTL) value.
ttl value [*value1* ... *value2*]	(Optional) TTL value used for filtering. Range is 1 to 255. If only *value* is specified, the match is against this value. If both *value1* and *value2* are specified, the packet TTL is matched against the range of TTLs between *value1* and *value2* .
icmp-type	(Optional) ICMP message type for filtering ICMP packets. Range is from 0 to 255.
icmp-code	(Optional) ICMP message code for filtering ICMP packets. Range is from 0 to 255.

igmp-type	(Optional) IGMP message type (0 to 15) or message name for filtering IGMP packets, as follows: • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • trace • v2-leave • v2-report • v3-report
operator	(Optional) Operator is used to compare source or destination ports. Possible operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard* values, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard* values, it must match the destination port. If the operator is positioned after the **ttl** keyword, it matches the TTL value. The **range** operator requires two port numbers. All other operators require one port number.
port	Decimal number a TCP or UDP port. Range is 0 to 65535. TCP ports can be used only when filtering TCP. UDP ports can be used only when filtering UDP.

protocol-port	Name of a TCP or UDP port. TCP and UDP port names are listed in the "Usage Guidelines" section. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection.
match-any	(Optional) For the TCP protocol only: Filters on any combination of TCP flags.
match-all	(Optional) For the TCP protocol only: Filters on all TCP flags.
+ | -	(Required) For the TCP protocol **match-any** , **match-all** : Prefix *flag-name* with **+** or **-** . Use the + *flag-name* argument to match packets with the TCP flag set. Use the - *flag-name* argument to match packets when the TCP flag is not set.
flag-name	(Optional) For the TCP protocol **match-any** , **match-all** . Flag names are: **ack** , **fin** , **psh** , **rst** , **syn** , **urg** .
counter	(Optional) Enables accessing ACL counters using SNMP query.
counter-name	Defines an ACL counter name.

Command Default

There is no specific condition under which a packet is denied passing the IPv4 access list.

ICMP message generation is enabled by default.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **permit** command following the **ipv4 access-list** command to specify conditions under which a packet can pass the access list.

By default, the first statement in an access list is number 10, and the subsequent statements are incremented by 10.

You can add **permit**, **deny**, or **remark** statements to an existing access list without retyping the entire list. To add a new **s**tatement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

The following is a list of precedence names:

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

The following is a list of ICMP message type names:

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-precedence-unreachable
- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem

- port-unreachable
- precedence-unreachable
- protocol-unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- traceroute
- ttl-exceeded
- unreachable

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec
- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- login
- lpd
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- tacacs
- talk

- telnet
- time
- uucp
- whois
- www

The following UDP port names can be used instead of port numbers. Refer to the current *Assigned Numbers* RFC to find a reference to these protocols. You can find port numbers corresponding to these protocols by typing a ? in the place of a port number.

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip
- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

Use the following flags in conjunction with the **match-any** and **match-all** keywords and the + and - signs to select the flags to display:

- ack
- fin
- psh
- rst
- syn

For example, **match-all** *+ack +syn* displays TCP packets with both the ack *and* syn flags set, or **match-any** *+ack* – - *syn* displays the TCP packets with the ack set *or* the syn not set.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

The following example shows how to set a permit condition for an access list named Internetfilter:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 permit 192.168.34.0 0.0.0.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit 172.16.0.0 0.0.255.255
RP/0/RP0/CPU0:router(config-ipv4-acl)# 25 permit tcp host 172.16.0.0 eq bgp host
192.168.202.203 range 1300 1400
RP/0/RP0/CPU0:router(config-ipv4-acl)# deny 10.0.0.0 0.255.255.255
```

remark (IPv4)

To write a helpful comment (remark) for an entry in an IPv4 access list, use the **remark** command in IPv4 access list configuration mode. To remove the remark, use the **no** form of this command.

[*sequence-number*] **remark** *remark*
no *sequence-number*

Syntax Description

sequence-number	(Optional) Number of the **remark** statement in the access list. This number determines the order of the statements in the access list. Range is 1 to 2147483646. (By default, the first statement is number 10; subsequent statements are incremented by 10.)
remark	Comment that describes the entry in the access list, up to 255 characters long.

Command Default

The IPv4 access list entries have no remarks.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **remark** command to write a helpful comment for an entry in an IPv4 access list. To remove the remark, use the **no** form of this command.

The remark can be up to 255 characters; anything longer is truncated.

If you know the sequence number of the remark you want to delete, you can remove it by entering the **no** *sequence-number* command.

Task ID

Task ID	Operations
ipv4	read, write
acl	read, write

Examples

In the following example, the user1 subnet is not allowed to use outbound Telnet:

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list telnetting
RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 deny tcp host 172.16.2.88 255.255.0.0 any eq
telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 30 permit icmp any any
RP/0/RP0/CPU0:router# show ipv4 access-list telnetting

ipv4 access-list telnetting
  0 remark Do not allow user1 to telnet out
```

```
20 deny tcp 172.16.2.88 255.255.0.0 any eq telnet out
30 permit icmp any any
```

resequence access-list ipv4

To renumber existing statements and increment subsequent statements to allow a new IPv4 access list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence access-list ipv4** command in XR EXEC mode.

resequence access-list ipv4 *name* [*base* [*increment*]]

Syntax Description

name	Name of an IPv4 access list.
base	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. Maximum value is 2147483644. Default is 10.
increment	(Optional) Number by which the base sequence number is incremented for subsequent statements. Maximum value is 2147483644. Default is 10.

Command Default

base: 10

increment: 10

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **resequence access-list ipv4** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv4 access list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software renumbers the existing statements, thereby making room to add new statements with the unused entry numbers.

Task ID

Task ID	Operations
acl	read, write

Examples

In this example, suppose you have an existing access list:

```
ipv4 access-list marketing
  1 permit 10.1.1.1
  2 permit 10.2.0.0 0.0.255.255
  3 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

You want to add additional entries in the access list. First you resequence the entries, renumbering the statements starting with number 20 and an increment of 5, and then you have room for four additional statements between each of the existing statements:

```
RP/0/RP0/CPU0:router# resequence access-list ipv4 marketing 20 5
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing
```

```
ipv4 access-list marketing
  20 permit 10.1.1.1
  25 permit 10.2.0.0
  30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

Now you add your new entries.

```
RP/0/RP0/CPU0:router(config)# ipv4 access-list marketing
RP/0/RP0/CPU0:router(config-ipv4-acl)# 3 remark Do not allow user1 to telnet out
RP/0/RP0/CPU0:router(config-ipv4-acl)# 4 deny tcp host 172.16.2.88 255.255.0.0 any eq telnet
RP/0/RP0/CPU0:router(config-ipv4-acl)# 29 remark Allow user2 to telnet out
RP/0/RP0/CPU0:router# show access-lists ipv4 marketing

ipv4 access-list marketing
  3 remark Do not allow user1 to telnet out
  4 deny tcp host 171.69.2.88 255.255.0.0 any eq telnet
  20 permit 10.1.1.1
  25 permit 10.2.0.0
  29 remark Allow user2 to telnet out
  30 permit tcp host 10.2.2.2 255.255.0.0 any eq telnet
```

show access-lists afi-all

To display the contents of current IPv4 and IPv6 access lists, use the **show access-lists afi-all** command in XR EXEC mode.

show access-lists afi-all

Syntax Description

This command has no keywords or arguments.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
acl	read

Examples

This sample output is from the **show access-lists afi-all** command:

```
RP/0/RP0/CPU0:router# show access-lists afi-all

ipv4 access-list crypto-1
 10 permit ipv4 65.21.21.0 0.0.0.255 65.6.6.0 0.0.0.255
 20 permit ipv4 192.168.241.0 0.0.0.255 192.168.65.0 0.0.0.255
```

show access-lists ipv4

To display the contents of current IPv4 access lists, use the **show access-lists ipv4** command in XR EXEC mode.

show access-lists ipv4 [{*access-list-name* **hardware** {**ingress**} [**interface** *type*] {**sequence** *number*|**location** *node-id*}|**summary** [*access-list-name*]|*access-list-name* [*sequence-number*]|**maximum** **[detail]** [**usage** **pfilter** { **location** *node-id* | **all**}]}]

Syntax Description

access-list-name	(Optional) Name of a particular IPv4 access list. The name cannot contain spaces or quotation marks, but can include numbers.
hardware	(Optional) Identifies the access list as an access list for an interface.
ingress	(Optional) Specifies an inbound interface.
interface	(Optional) Displays interface statistics.
type	(Optional) Interface type. For more information, use the question mark (?) online help function.
sequence *number*	(Optional) Sequence number of a particular IPv4 access list. Range is 1 to 2147483644.
location *node-id*	(Optional) Location of a particular IPv4 access list. The *node-id* argument is entered in the *rack/slot/module* notation.
summary	(Optional) Displays a summary of all current IPv4 access lists.
sequence-number	(Optional) Sequence number of a particular IPv4 access list. Range is 1 to 2147483644.
maximum	(Optional) Displays the current maximum number of configurable IPv4 access control lists (ACLs) and access control entries (ACEs).
detail	(Optional) Displays complete out-of-resource (OOR) details.

usage	(Optional) Displays the usage of the access list on a given line card.
pfilter	(Optional) Displays the packet filtering usage for the specified line card.
all	(Optional) Displays the location of all the line cards.

Command Default

The default displays all IPv4 access lists.

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

Use the **show access-lists ipv4** command to display the contents of all IPv4 access lists. To display the contents of a specific IPv4 access list, use the *name* argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **hardware , ingress** and **location** keywords to display the access list hardware contents and counters for all interfaces that use the specified access list in a given direction. To display the contents of a specific access list entry, use the **sequence** *number* keyword and argument. The access group for an interface must be configured using the **ipv4 access-group** command for access list hardware counters to be enabled.

Use the **show access-lists ipv4 summary** command to display a summary of all current IPv4 access lists. To display a summary of a specific IPv4 access list, use the *name* argument.

Use the **show access-lists ipv4 maximum detail** command to display the OOR details for IPv4 access lists. OOR limits the number of ACLs and ACEs that can be configured in the system. When the limit is reached, configuration of new ACLs or ACEs is rejected.

Use the **show access-list ipv4 usage** command to display a summary of all interfaces and access lists programmed on the specified line card.

ACL on **egress** is not supported in Release 6.0

Task ID

Task ID	Operations
acl	read

Examples

In the following example, the contents of all IPv4 access lists are displayed:

```
RP/0/RP0/CPU0:router# show access-lists ipv4

ipv4 access-list 101
  10 deny udp any any eq ntp
  20 permit tcp any any
  30 permit udp any any eq tftp
  40 permit icmp any any
  50 permit udp any any eq domain
ipv4 access-list Internetfilter
  10 permit tcp any 172.16.0.0 0.0.255.255 eq telnet
  20 deny tcp any any
  30 deny udp any 172.18.0.0 0.0.255.255 lt 1024
  40 deny ipv4 any any log
```

This table describes the significant fields shown in the display.

Table 1: show access-lists ipv4 hardware Field Descriptions

Field	Description
hw matches	Number of hardware matches.
ACL name	Name of the ACL programmed in hardware.
Sequence Number	Each ACE sequence number is programmed into hardware with all the fields that are corresponding to the values set in ACE.
Grant	Depending on the ACE rule, the grant is set to deny, permit, or both.
Logging	Logging is set to on if ACE uses a log option to enable logs.
Per ace icmp	If Per ace icmp is set to on in the hardware, ICMP is unreachable, is rate-limited, and is generated. The default is set to on.
Hits	Hardware counter for that ACE.

In the following example, a summary of all IPv4 access lists are displayed:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 summary

ACL Summary:
  Total ACLs configured: 3
  Total ACEs configured: 11
```

This table describes the significant fields shown in the display.

Table 2: show access-lists ipv4 summary Field Descriptions

Field	Description
Total ACLs configured	Number of configured IPv4 ACLs.
Total ACEs configured	Number of configured IPV4 ACEs.

In the following example, the OOR details of the IPv4 access lists are displayed:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 maximum detail

Default max configurable acls :5000
Default max configurable aces :200000
Current configured acls       :1
Current configured aces       :2
Current max configurable acls :5000
Current max configurable aces :200000
Max configurable acls         :9000
Max configurable aces         :350000
```

This table describes the significant fields shown in the display.

Table 3: show access-lists ipv4 maximum detail Command Field Descriptions

Field	Description
Default max configurable acls	Default maximum number of configurable IPv4 ACLs allowed.
Default max configurable aces	Default maximum number of configurable IPv4 ACEs allowed.
Current configured acls	Number of configured IPv4 ACLs.
Current configured aces	Number of configured IPv4 ACEs.
Current max configurable acls	Configured maximum number of configurable IPv4 ACLs allowed.
Current max configurable aces	Configured maximum number of configurable IPv4 ACEs allowed.
Max configurable acls	Maximum number of configurable IPv4 ACLs allowed.
Max configurable aces	Maximum number of configurable IPv4 ACEs allowed.

This example displays the packet filtering usage for the specified line card:

```
RP/0/RP0/CPU0:router# show access-lists ipv4 usage pfilter location 0/RP0/CPU0

Interface : tenGigE 0/0/0/1
Input Common-ACL : ipv4_c_acl  ACL : ipv4_i_acl_1
Output ACL : ipv4_i_acl_1
```

Note To display the packet filtering usage for bundle interfaces, use the **show access-lists ipv4 usage pfilter location all** command.

show pfilter-ea

To display the packet filter-ea information, enter the show pfilter-ea command in XR EXEC mode on the ASR 9000 Enhanced Ethernet line card.

show pfilter-ea fea {**ipv4-acl | ipv6-acl** } *acl-name* **location** *node-id*

Syntax Description

ipv4-acl	Indicates IPv4 access lists.
ipv6-acl	Indicates IPv6 access lists.
acl-name	Name of the IPv4/IPv6 access list.
location *node-id*	Location of a particular IPv4/IPv6 access list. The node-id argument is entered in the rack/slot/module notation.

Command Default

None

Command Modes

XR EXEC mode

Command History

Release	Modification
Release 6.0	This command was introduced.

Usage Guidelines

This command is available only on the ASR 9000 Enhanced Ethernet line card.

Task ID

Task ID	Operation
root-system	read, write

Example

This example shows how to display the packet filter-ea information:

```
RP/0/RP0/CPU0:router#  show feature-mgr client pfilter-ea feature-info summary location
0/RP0/CPU0

IFH        NPU DIR Lookup-type  VMR-ID      ACL-ID Refcnt Feature-Name
---------- --- --- -----------  ----------- ------ ------ ------------
0x8000048  0   IN  IPV4_ACL (L3) 0x2          3      1      skywarp_acl
0x8000038  0   IN  IPV4_ACL (L3) 0x1          2      1      v4-acl
0x8000040  0   IN  IPV4_ACL (L2) 0x200000001  2      1      v4-acl
```

This table describes the significant fields shown in the display.

Table 4: show pfilter-ea Field Descriptions

Field	Description
IFH	Interface Handle of the interface on which the ACL is Applied.
DIR	Indicates the direction in which ACL is applied. IN for ingress and OUT for egress.
Lookup-type	Indicated the the type of ACL, either IPV4 or IPV6. L3/L2 indicate the interface type.
Reference count	Indicates the Number of interface a particular ACL is applied.
Feature name	Name of the ACL programmed in hardware.