



Access List Commands on Cisco IOS-XR Software

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

An access control list (ACL) consists of one or more access control entries (ACEs) that collectively define the network traffic profile. This profile can then be referenced by Cisco IOS-XR software features such as traffic filtering, priority or custom queueing, and dynamic access control. Each ACL includes an action element (permit or deny) and a filter element based on criteria such as source address, destination address, protocol, and protocol-specific parameters.

For detailed information about ACL concepts, configuration tasks, and examples, refer to the *Cisco IOS-XR IP Addresses and Services Configuration Guide*.

clear ipv4 access-list

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

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

Syntax Description

<i>access-list-name</i>	Name of a particular IPv4 access list. The name cannot contain a space or quotation mark; it may contain numbers.
sequence number	(Optional) Clears counters for an access list with a specific sequence number. Value is from 1 to 2147483646.
hardware	Identifies the access list as an access group for an interface.
ingress	Specifies an inbound direction.
egress	Specifies an outbound direction.
location <i>node-id</i>	Clears counters for an access list enabled on a card interface. The <i>node-id</i> argument is entered in the rack/slot/module notation.
<i>sequence-number</i>	(Optional) Clears counters for an access list with a specific sequence number. Value is from 1 to 2147483646.

Defaults

Clears a specified IPv4 access list.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **clear ipv4 access-list** 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 the **hardware** keyword to clear counters for an access list that was enabled using the **ipv4 access-group** command.

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



Note

An access list can be shared among multiple interfaces. Clearing hardware counters clears all counters for all interfaces that use the specified access list in a given direction (ingress or egress).

Examples

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

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

ipv4 access-list marketing
 10 permit ip 192.168.34.0 0.0.0.255 any (51 matches)
 20 permit ip 172.16.0.0 0.0.255.255 any (26 matches)
 30 deny tcp host 172.16.0.0 eq bgp host 192.168.202.203 30 (5 matches)

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

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

In the following example, counters for an access list named *acl_hw_1* in the outbound direction are cleared:

```
RP/0/RP0/CPU0:router# show ipv4 access-lists acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
 10 permit icmp 192.168.36.0 0.0.0.255 any (251 hw matches)
 20 permit ip 172.16.3.0 0.0.255.255 any (29 hw matches)
 30 deny tcp any any (58 hw matches)

RP/0/RP0/CPU0:router# clear ipv4 access-list acl_hw_1 hardware egress location 0/2/cp0

RP/0/RP0/CPU0:router# show ipv4 access-lists acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
 10 permit icmp 192.168.36.0 0.0.0.255 any
 20 permit ip 172.16.3.0 0.0.255.255 any
 30 deny tcp any any
```

Related Commands

Command	Description
ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
show ipv4 access-lists	Displays the contents of all current IPv4 access lists.

clear ipv6 access-list

To clear IPv6 access list counters, use the **clear ipv6 access-list** command in EXEC mode.

```
clear ipv6 access-list access-list-name [hardware {ingress | egress}] {sequence number | location node-id} | sequence-number
```

Syntax Description

<i>access-list-name</i>	Name of a particular IPv6 access list. The name cannot contain a space or quotation mark; it may contain numbers.
sequence number	(Optional) Clears counters for an access list with a specific sequence number. Value is from 1 to 2147483646.
hardware	Identifies the access list as an access group for an interface.
ingress	Specifies an inbound direction.
egress	Specifies an outbound direction.
location <i>node-id</i>	Clears counters for an access list enabled on a card interface. The <i>node-id</i> argument is entered in the rack/slot/module notation.
<i>sequence-number</i>	(Optional) Clears counters for an access list with a specific sequence number. Value is from 1 to 2147483646.

Defaults

Clears a specified IPv6 access list.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **clear ipv6 access-list** command is similar to the **clear ipv4 access-list** command, except that it is IPv6-specific.

Use the **clear ipv6 access-list** 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 the **hardware** keyword to clear counters for an access list that was enabled using the **ipv6 access-group** command.

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



Note

An access list can be shared among multiple interfaces. Clearing hardware counters clears all counters for all interfaces that use the specified access list in a given direction (ingress or egress).

Examples

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

```
RP/0/RP0/CPU0:router# show ipv6 access-lists marketing

ipv6 access-list marketing
 10 permit ipv6 3333:1:2:3::/64 any (51 matches)
 20 permit ipv6 4444:1:2:3::/64 any (26 matches)
 30 permit ipv6 5555:1:2:3::/64 any (5 matches)

RP/0/RP0/CPU0:router# clear ipv6 access-list marketing

RP/0/RP0/CPU0:router# show ipv6 access-lists marketing

ipv6 access-list marketing
 10 permit ipv6 3333:1:2:3::/64 any
 20 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
```

In the following example, counters for an access list named *acl_hw_1* in the outbound direction are cleared:

```
RP/0/RP0/CPU0:router# show ipv6 access-lists acl_hw_1 hardware egress location 0/2/cp0

ipv6 access-list acl_hw_1
 10 permit ipv6 3333:1:2:3::/64 any (251 hw matches)
 20 permit ipv6 4444:1:2:3::/64 any (29 hw matches)
 30 deny tcp any any (58 hw matches)

RP/0/RP0/CPU0:router# clear ipv6 access-list acl_hw_1 hardware egress location 0/2/cp0

RP/0/RP0/CPU0:router# show ipv6 access-lists acl_hw_1 hardware egress location 0/2/cp0

ipv6 access-list acl_hw_1
 10 permit ipv6 3333:1:2:3::/64 any
 20 permit ipv6 4444:1:2:3::/64 any
 30 deny tcp any any
```

Related Commands

Command	Description
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.

copy ipv4 access-list

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

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

Syntax Description	
<i>source-acl</i>	Name of the access list to be copied.
<i>destination-acl</i>	Destination access list where the contents of the <i>source-acl</i> argument will be copied.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **copy ipv4 access-list** 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 ipv4 access-list** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists or prefix lists.

Examples

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

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

ipv4 access-list list-1
 10 permit tcp any any log
 20 permit ip any any
RP/0/RP0/CPU0:router# copy ipv4 access-list list-1 list-2
RP/0/RP0/CPU0:router# show ipv4 access-lists 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 ipv4 access-list list-1 list-3

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

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

Related Commands	Command	Description
	ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
	show ipv4 access-lists	Displays the contents of all current IPv4 access lists.

copy ipv6 access-list

To create a copy of an existing IPv6 access list, use the **copy ipv6 access-list** command in EXEC mode.

```
copy ipv6 access-list source-acl destination-acl
```

Syntax Description	
<i>source-acl</i>	Name of the access list to be copied.
<i>destination-acl</i>	Destination access list where the contents of the <i>source-acl</i> argument will be copied.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **copy ipv6 access-list** 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 ipv6 access-list** command checks that the source access list exists then checks the existing list names to prevent overwriting existing access lists or prefix lists.

Examples

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

```
RP/0/RP0/CPU0:router# show ipv6 access-list list-1

ipv6 access-list list-1
 10 permit tcp any any log
 20 permit ipv6 any any

RP/0/RP0/CPU0:router# copy ipv6 access-list list-1 list-2
RP/0/RP0/CPU0:router# show ipv6 access-lists list-2

ipv6 access-list list-2
 10 permit tcp any any log
 20 permit ipv6 any any
```

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

```
RP/0/RP0/CPU0:router# copy ipv6 access-list list-1 list-3

list-3 exists in access-list
```

```
RP/0/RP0/CPU0:router# show ipv6 access-lists list-3
```

```
ipv6 access-list list-3
 10 permit ipv6 any any
 20 deny tcp any any log
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.

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] [log | log-input]
```

```
[sequence-number] deny protocol source source-wildcard destination destination-wildcard
[precedence precedence] [dscp dscp] [fragments] [log | log-input]
```

```
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 | log-input]
```

Internet Group Management Protocol (IGMP)

```
[sequence-number] deny igmp source source-wildcard destination destination-wildcard
[igmp-type] [precedence precedence] [dscp value] [fragments] [log | log-input]
```

Stream Control Transmission Protocol (SCTP)

```
[sequence-number] deny sctp source source-wildcard [operator {port | protocol-port}] destination
destination-wildcard [operator {port | protocol-port}] [established] [ack] [rst] [syn] [fin]
[push] [precedence precedence] [dscp dscp] [fragments] [log | log-input]
```

Transmission Control Protocol (TCP)

```
[sequence-number] deny tcp source source-wildcard [operator {port | protocol-port}] destination
destination-wildcard [operator {port | protocol-port}] [established] [ack] [rst] [syn] [fin]
[push] [precedence precedence] [dscp dscp] [fragments] [log | log-input]
```

User Datagram Protocol (UDP)

```
[sequence-number] deny udp source source-wildcard [operator {port | protocol-port}] destination
destination-wildcard [operator {port | protocol-port}] [precedence precedence] [dscp dscp]
[fragments] [log | log-input]
```

Syntax Description	
<i>sequence-number</i>	(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 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the resequence access-list command to change the number of the first statement and increment subsequent statements of a configured access list.
<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted-decimal format. • Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use the host source combination as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none"> • 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use the host source combination as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords ahp , esp , eigrp , gre , icmp , igmp , igrp , ip , ipinip , nos , ospf , pim , pcp , sctp , 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, SCTP, and TCP allow further qualifiers, which are described later in this table.
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted-decimal format. • Use the any keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use the host destination combination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: <ul style="list-style-type: none"> • 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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use the host destination combination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.

precedence <i>precedence</i>	<p>(Optional) Packets can be filtered by precedence level (as specified by a number from 0 to 7) or by the following names:</p> <ul style="list-style-type: none"> • match—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 <i>dscp</i>	<p>(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for <i>dscp</i> are as follows:</p> <ul style="list-style-type: none"> • 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	<p>(Optional) Causes the software to examine non initial fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.</p>

log	<p>(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.)</p> <p>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.</p>
log-input	(Optional) Provides the same function as the log keyword, except that the logging message also includes the input interface.
<i>icmp-type</i>	(Optional) ICMP packets are filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(Optional) ICMP packets are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
<i>igmp-type</i>	<p>(Optional) IGMP packets are filtered by IGMP message type (0 to 15) or message name, as follows:</p> <ul style="list-style-type: none"> • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • trace • v2-leave • v2-report • v3-report
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i> values, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i> values, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>
<i>port</i>	<p>The decimal number a TCP or UDP port. A port number is a number from 0 to 65535.</p> <p>TCP ports can be used only when filtering TCP. UDP ports can be used only when filtering UDP.</p>

<i>protocol-port</i>	The 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. A match occurs if the TCP datagram has the Acknowledgment (ACK) or Reset (RST) bit set. The nonmatching case is that of the initial TCP datagram to form a connection.
ack	(Optional) For the TCP protocol only: ACK bit set.
rst	(Optional) For the TCP protocol only: RST bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
psh	(Optional) For the TCP protocol only: Push function bit set.

Defaults

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

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.

If you want to add a statement between two consecutively numbered statements (for example, between lines 10 and 11), first use the **resequence access-list** command to renumber the first statement and increment the entry number of each subsequent statement. The *increment* argument causes new, unused line numbers between statements. Then add a new statement with the *entry-number* specifying where it belongs in the access list.

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**

- **reassemble-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**

Examples

The following example sets a deny 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 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
```

Related Commands

Command	Description
ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets conditions under which a packet passes a named IPv4 access list.
remark (IPv4)	Inserts a helpful remark about an IPv4 access list entry.
resequence ipv4 access-list	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.
show ipv4 access-lists	Displays the contents of all current IPv4 access lists.

deny (IPv6)

To set deny conditions for an IPv6 access list, use the **deny** command in IPv6 access list configuration mode. To remove the deny conditions, use the **no** form of this command.

```
[sequence-number] deny protocol {source-ipv6-prefix/prefix-length | any | host
source-ipv6-address} [operator {port | protocol-port}] {destination-ipv6-prefix/prefix-length |
any | host destination-ipv6-address} [operator {port | protocol-port}] [dscp value] [routing]
[authen] [destopts] [fragments] [log] [log-input]
```

```
no sequence-number
```

Internet Control Message Protocol (ICMP)

```
[sequence-number] deny icmp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
{destination-ipv6-prefix/prefix-length | any | host destination-ipv6-address} [icmp-type]
[icmp-code] [dscp value] [routing] [authen] [destopts] [fragments] [log] [log-input]
```

Transmission Control Protocol (TCP)

```
[sequence-number] deny tcp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[operator {port | protocol-port}] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address} [operator {port | protocol-port}] [dscp value] [routing] [authen]
[destopts] [fragments] [established] [ack] [fin] [psh] [rst] [syn] [log] [log-input]
```

User Datagram Protocol (UDP)

```
[sequence-number] deny udp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[operator {port | protocol-port}] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address} [operator {port | protocol-port}] [dscp value] [routing] [authen]
[destopts] [fragments] [log] [log-input]
```

Syntax Description

<i>sequence-number</i>	(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 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the resequence access-list command to change the number of the first statement and increment subsequent statements of a configured access list.
<i>protocol</i>	Name or number of an Internet protocol. It can be one of the keywords ahp , esp , icmp , ipv6 , pcp , sctp , tcp , or udp , or an integer in the range from 0 to 255 representing an IPv6 protocol number.
<i>source-ipv6-prefix/prefix-length</i>	The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix <code>::/0</code> .

host <i>source-ipv6-address</i>	The source IPv6 host address about which to set deny conditions. This <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>operator</i> { <i>port</i> <i>protocol-port</i> }	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). If the operator is positioned after the <i>source-ipv6-prefix/prefix-length</i> argument, it must match the source port. If the operator is positioned after the <i>destination-ipv6-prefix/prefix-length</i> argument, it must match the destination port. The range operator requires two port numbers. All other operators require one port number. The <i>port</i> argument is the decimal number of a TCP or UDP port. A port number is a number from 0 to 65535. The <i>protocol-port</i> argument is the name of a TCP or UDP port. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
<i>destination-ipv6-prefix/prefix-length</i>	The destination IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host <i>destination-ipv6-address</i>	The destination IPv6 host address about which to set deny conditions. This <i>destination-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dscp <i>value</i>	(Optional) Matches a differentiated services code point DSCP value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
authen	(Optional) Matches if the IPv6 authentication header is present.
destopts	(Optional) Matches if the IPv6 destination options header is present.
fragments	(Optional) Matches noninitial fragmented packets where the fragment extension header contains a nonzero fragment offset. The fragments keyword is an option only if the <i>operator</i> [<i>port-number</i>] arguments are not specified.

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 name and sequence number, whether the packet was 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, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the log keyword, except that the logging message also includes the input interface.
<i>icmp-type</i>	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the Acknowledgement (ACK) or Reset (RST) bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
ack	(Optional) For the TCP protocol only: ACK bit set.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
psh	(Optional) For the TCP protocol only: Push function bit set.
rst	(Optional) For the TCP protocol only: RST bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.

Defaults

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **deny** (IPv6) command is similar to the **deny** (IPv4) command, except that it is IPv6-specific.

Use the **deny** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list.

Specifying **ipv6** for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 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.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

**Note**

IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator {port | protocol-port}* arguments are not specified.

Examples

The following example configures the IPv6 access list named toCISCO and applies the access list to outbound traffic on packet over SONET (POS) interface 0/2/0/2. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of POS interface 0/2/0/2. The second deny entry in the list keeps all packets that have a source UDP port number less than 5000 from exiting out of POS interface 0/2/0/2. The second deny entry also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of POS interface 0/2/0/2. The second permit entry in the list permits all other traffic to exit out of POS interface 0/2/0/2. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list toCISCO

RP/0/RP0/CPU0:router(config-ipv6-acl)# deny tcp any any gt 5000
RP/0/RP0/CPU0:router(config-ipv6-acl)# deny ipv6 any lt 5000 any log
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit icmp any any
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit any any

RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group toCISCO out
```

Related Commands

Command	Description
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
remark (IPv6)	Inserts a helpful remark about an IPv6 access list entry.
resequence ipv6 access-list	Changes the starting entry number of the first statement in an existing IPv6 access list, and the number by which subsequent statements are incremented.
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.

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 {in | out} [hw-count]
```

```
no ipv4 access-group access-list-name {in | out} [hw-count]
```

Syntax Description

<i>access-list-name</i>	Name of an IPv4 access list as specified by an ipv4 access-list command.
in	Filters on inbound packets.
out	Filters on outbound packets.
<i>hw-count</i>	(Optional) Enables hardware counters for an access group.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 **in** keyword to filter on inbound packets or the **out** keyword to filter on outbound packets. Use the *hw-count* argument to enable hardware counters for the access group.

Permitted packets are counted only when hardware counters are enabled using the *hw-count* argument. Denied packets are counted whether hardware counters are enabled or not.



Note

For packet filtering applications using the **ipv4 access-group** command, packet counters are maintained in hardware for each direction. If an access group is used on multiple interfaces in the same direction, then packets are counted for each interface that has the *hw-count* argument enabled.

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.

Examples

The following example applies filters on packets inbound and outbound from packet over SONET (POS) interface 0/2/0/2:

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

Related Commands

Command	Description
clear ipv4 access-list	Resets the IPv4 access list match counters.
deny (IPv4)	Sets conditions under which a packet does not pass a named IPv4 access list.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets conditions under which a packet passes a named IPv4 access list.
show ipv4 access-lists	Displays the contents of all current IPv4 access lists.
show ipv4 interface	Displays the status and configuration for a specified interface including the inbound and outbound access lists that are applied to the interface.

ipv4 access-list

To define an IPv4 access list by name, use the **ipv4 access-list** command in global configuration 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	<i>name</i>
	Name of the access list. Names cannot contain a space or quotation marks.

Defaults	No IPv4 access list is defined.
----------	---------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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

Use the **resequence ipv4 access-list** command if you want 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 will renumber the existing statements, thereby making room to add new statements with the unused entry numbers.

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

Examples

The following example defines a standard access list named Internetfilter:

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

Related Commands	Command	Description
	clear ipv4 access-list	Resets the IPv4 access list match counters.
	deny (IPv4)	Sets conditions for a named IPv4 access list.
	ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
	permit (IPv4)	Sets conditions for a named IPv4 access list.
	remark (IPv4)	Inserts a helpful remark about an IPv4 access list entry.
	resequence ipv4 access-list	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.
	show ipv4 access-lists	Displays the contents of all current IPv4 access lists.

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 global configuration 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

<i>update-number</i>	Specifies the number of updates that are logged for every IPv4 access list configured on the router. The acceptable range is from 0 to 2147483647.
----------------------	--

Defaults

For IPv4 access lists, 2147483647 updates are logged.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.

Examples

The following example configures 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
```

Related Commands

Command	Description
deny (IPv4)	Sets deny conditions for an IPv4 access list.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets conditions under which a packet passes a named IPv4 access list.
show ipv4 access-lists	Displays the contents of all current IPv4 access lists.

ipv6 access-group

To control access to an interface, use the **ipv6 access-group** command in interface configuration mode. To remove the specified access group, use the **no** form of this command.

ipv6 access-group *access-list-name* { **in** | **out** }

no ipv6 access-group *access-list-name* { **in** | **out** }

Syntax Description

<i>access-list-name</i>	Name of an IPv6 access list as specified by an ipv6 access-list command.
in	Filters on inbound packets.
out	Filters on outbound packets.

Defaults

The interface does not have an IPv6 access list applied to it.

Command Modes

Interface configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **ipv6 access-group** command is similar to the **ipv4 access-group** command, except that it is IPv6-specific.

Use the **ipv6 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* to specify a particular IPv6 access list. Use the **in** keyword to filter on inbound packets or the **out** keyword to filter on outbound packets.



Note

For packet filtering applications using the **ipv6 access-group** command, packet counters are maintained in hardware for each direction. If an access group is used on multiple interfaces in the same direction, then packets are counted for each interface.

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 a rate-limited Internet Control Message Protocol (ICMP) host unreachable message.

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

Examples

The following example applies filters on packets inbound and outbound from packet over SONET (POS) interface 0/2/0/2:

```
RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group p-in-filter in
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group p-out-filter out
```

Related Commands

Command	Description
copy ipv6 access-list	Resets the IPv6 access list match counters.
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets conditions under which a packet passes a named IPv6 access list.
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.
show ipv6 interface	Displays the status and configuration for a specified interface including the inbound and outbound access-lists that are applied to the interface.

ipv6 access-list

To define an IPv6 access list and to place the router in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *name*

no ipv6 access-list *name*

Syntax Description

<i>name</i>	Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
-------------	--

Defaults

No IPv6 access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **ipv6 access-list** command is similar to the **ipv4 access-list** command, except that it is IPv6-specific. The IPv6 access lists are used for traffic filtering based on source and destination addresses, IPv6 option headers, and optional, upper-layer protocol type information for finer granularity of control. IPv6 access lists are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list** command places the router in IPv6 access list configuration mode—the router prompt changes to router(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 access list.

Refer to the **deny** (IPv6) and **permit** (IPv6) commands for more information on filtering IPv6 traffic based on IPv6 option headers and optional, upper-layer protocol type information. See the “Examples” section for an example of a translated IPv6 access control list (ACL) configuration.



Note

Every IPv6 access list has an implicit **deny ipv6 any any** statement as its last match condition. An IPv6 access list must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect.



Note

IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

Use the **ipv6 access-group** interface configuration command with the *access-list-name* argument to apply an IPv6 access list to an IPv6 interface.

**Note**

An IPv6 access list applied to an interface with the **ipv6 access-group** command filters traffic that is forwarded, not originated, by the router.

Examples

The following example configures the IPv6 access list named list2 and applies the ACL to outbound traffic on interface packet over SONET (POS) 0/2/0/2. Specifically, the first ACL entry keeps all packets from the network fec0:0:0:2::/64 (packets that have the site-local prefix fec0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of interface POS 0/2/0/2. The second entry in the ACL permits all other traffic to exit out of interface POS 0/2/0/2. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list list2

RP/0/RP1/CPU0:router(config-ipv6-acl)# 10 deny fec0:0:0:2::/64 any
RP/0/RP1/CPU0:router(config-ipv6-acl)# 20 permit any any

RP/0/RP1/CPU0:router# show ipv6 access-lists list2

ipv6 access-list list2
 10 deny ipv6 fec0:0:0:2::/64 any
 20 permit ipv6 any any

RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2

RP/0/RP0/CPU0:router(config-if)# ipv6 access-group list2 out
```

**Note**

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

**Note**

An IPv6 router will not forward to another network an IPv6 packet that has a link-local address as either its source or destination address (and the source interface for the packet is different from the destination interface for the packet).

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
remark (IPv6)	Inserts a helpful remark about an IPv6 access list entry.
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.

ipv6 access-list log-update threshold

To specify the number of updates that are logged for IPv6 access lists, use the **ipv6 access-list log-update threshold** command in global configuration mode. To return the number of logged updates to the default setting, use the **no** form of this command.

ipv6 access-list log-update threshold *update-number*

no ipv6 access-list log-update threshold *update-number*

Syntax Description

<i>update-number</i>	Specifies the number of updates that are logged for every IPv6 access list configured on the router. The acceptable range is from 0 to 2147483647.
----------------------	--

Defaults

For IPv6 access lists, 2147483647 updates are logged.

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **ipv6 access-list log-update threshold** command is similar to the **ipv4 access-list log-update threshold** command, except that it is IPv6-specific.

IPv6 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.

Examples

The following example configures a log threshold of ten updates for every IPv6 access list configured on the router:

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list log-update threshold 10
```

Related Commands

Command	Description
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.

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 | log-input]
```

```
[sequence-number] permit protocol source source-wildcard destination destination-wildcard
[precedence precedence] [dscp dscp] [fragments] [log | log-input]
```

```
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] [log | log-input]
```

Internet Group Management Protocol (IGMP)

```
[sequence-number] permit igmp source source-wildcard destination destination-wildcard
[igmp-type] [precedence precedence] [dscp value] [fragments] [log | log-input]
```

Stream Control Transmission Protocol (SCTP)

```
[sequence-number] permit sctp source source-wildcard [operator {port | protocol-port}]
destination destination-wildcard [operator {port | protocol-port}] [established] [ack] [rst]
[syn] [fin] [psh] [precedence precedence] [dscp dscp] [fragments] [log | log-input]
```

Transmission Control Protocol (TCP)

```
[sequence-number] permit tcp source source-wildcard [operator {port | protocol-port}]
destination destination-wildcard [operator {port | protocol-port}] [established] [ack] [rst]
[syn] [fin] [psh] [precedence precedence] [dscp dscp] [fragments] [log | log-input]
```

User Datagram Protocol (UDP)

```
[sequence-number] permit udp source source-wildcard [operator {port | protocol-port}]
destination destination-wildcard [operator {port | protocol-port}] [precedence precedence]
[dscp dscp] [fragments] [log | log-input]
```

Syntax Description

<i>sequence-number</i>	(Optional) Number of the permit statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the resequence access-list command to change the number of the first statement and increment subsequent statements of a configured access list.
<i>source</i>	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted-decimal format. • Use the any keyword as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use the host source combination as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>source-wildcard</i>	Wildcard bits to be applied to the source. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none"> • 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 <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use the host source combination as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords ahp , esp , eigrp , gre , icmp , igmp , igrp , ip , ipinip , nos , ospf , pim , pcp , sctp , 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, SCTP, and TCP allow further qualifiers, which are described later in this table.
<i>destination</i>	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part dotted-decimal format. • Use the any keyword as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use the host destination combination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.
<i>destination-wildcard</i>	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: <ul style="list-style-type: none"> • 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 <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use the host destination combination as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of <i>destination</i> 0.0.0.0.

precedence <i>precedence</i>	<p>(Optional) Packets can be filtered by precedence level (as specified by a number from 0 to 7) or by the following names:</p> <ul style="list-style-type: none"> • match—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 <i>dscp</i>	<p>(Optional) Differentiated services code point (DSCP) provides quality of service control. The values for <i>dscp</i> are as follows:</p> <ul style="list-style-type: none"> • 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	<p>(Optional) Causes the software to examine non initial fragments of IPv4 packets when applying this access list entry. When this keyword is specified, fragments are subject to the access list entry.</p>

log	<p>(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.)</p> <p>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.</p>
log-input	(Optional) Provides the same function as the log keyword, except that the logging message also includes the input interface.
<i>icmp-type</i>	(Optional) ICMP packets are filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(Optional) ICMP packets are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
<i>igmp-type</i>	<p>(Optional) IGMP packets are filtered by IGMP message type (0 to 15) or message name, as follows:</p> <ul style="list-style-type: none"> • dvmrp • host-query • host-report • mtrace • mtrace-response • pim • precedence • trace • v2-leave • v2-report • v3-report
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).</p> <p>If the operator is positioned after the <i>source</i> and <i>source-wildcard</i> values, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i> values, it must match the destination port.</p> <p>The range operator requires two port numbers. All other operators require one port number.</p>
<i>port</i>	<p>The decimal number a TCP or UDP port. A port number is a number from 0 to 65535.</p> <p>TCP ports can be used only when filtering TCP. UDP ports can be used only when filtering UDP.</p>

<i>protocol-port</i>	The 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. A match occurs if the TCP datagram has the Acknowledgment (ACK) or Reset (RST) bit set. The nonmatching case is that of the initial TCP datagram to form a connection.
ack	(Optional) For the TCP protocol only: ACK bit set.
rst	(Optional) For the TCP protocol only: RST bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
psh	(Optional) For the TCP protocol only: Push function bit set.

Defaults

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

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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 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.

If you want to add a statement between two consecutively numbered statements (for example, between lines 10 and 11), first use the **resequence access-list** command to renumber the first statement and increment the entry number of each subsequent statement. The *increment* argument causes new, unused line numbers between statements. Then add a new statement with the *entry-number* specifying where it belongs in the access list.

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**

- **reassemble-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**

Examples

The following example sets 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
```

Related Commands

Command	Description
deny (IPv4)	Sets conditions under which a packet does not pass a named IPv4 access list.
ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
remark (IPv4)	Inserts a helpful remark about an IPv4 access list entry.
resequence ipv4 access-list	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.
show ipv4 access-lists	Displays the contents of all current IPv4 access lists.

permit (IPv6)

To set permit conditions for an IPv6 access list, use the **permit** command in IPv6 access list configuration mode. To remove the permit conditions, use the **no** form of this command.

```
[sequence-number] permit protocol {source-ipv6-prefix/prefix-length | any | host
source-ipv6-address} [operator {port | protocol-port}] {destination-ipv6-prefix/prefix-length |
any | host destination-ipv6-address} [operator {port | protocol-port}] [dscp value] [routing]
[authen] [destopts] [fragments] [log] [log-input]
```

```
no sequence-number
```

Internet Control Message Protocol (ICMP)

```
[sequence-number] permit icmp {source-ipv6-prefix/prefix-length | any | host
source-ipv6-address} {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address} [icmp-type] [icmp-code] [dscp value] [routing] [authen] [destopts]
[fragments] [log] [log-input]
```

Transmission Control Protocol (TCP)

```
[sequence-number] permit tcp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[operator {port | protocol-port}] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address} [operator {port | protocol-port}] [dscp value] [routing] [authen]
[destopts] [fragments] [established] [ack] [fin] [psh] [rst] [syn] [log] [log-input]
```

User Datagram Protocol (UDP)

```
[sequence-number] permit udp {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
[operator {port | protocol-port}] {destination-ipv6-prefix/prefix-length | any | host
destination-ipv6-address} [operator {port | protocol-port}] [dscp value] [routing] [authen]
[destopts] [fragments] [log] [log-input]
```

Syntax Description		
<i>sequence-number</i>		(Optional) Number of the permit statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.) Use the resequence access-list command to change the number of the first statement and increment subsequent statements of a configured access list.
<i>protocol</i>		Name or number of an Internet protocol. It can be one of the keywords ahp , esp , icmp , ipv6 , pcp , sctp , tcp , or udp , or an integer in the range from 0 to 255 representing an IPv6 protocol number.
<i>source-ipv6-prefix/prefix-length</i>		The source IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any		An abbreviation for the IPv6 prefix ::/0 .

host <i>source-ipv6-address</i>	The source IPv6 host address about which to set permit conditions. This <i>source-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>operator</i> { <i>port</i> <i>protocol-port</i> }	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range). If the operator is positioned after the <i>source-ipv6-prefix/prefix-length</i> argument, it must match the source port. If the operator is positioned after the <i>destination-ipv6-prefix/prefix-length</i> argument, it must match the destination port. The range operator requires two port numbers. All other operators require one port number. The <i>port</i> argument is the decimal number of a TCP or UDP port. A port number is a number from 0 to 65535. The <i>protocol-port</i> argument is the name of a TCP or UDP port. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
<i>destination-ipv6-prefix/</i> <i>prefix-length</i>	The destination IPv6 network or class of networks about which to set permit conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host <i>destination-ipv6-address</i>	The destination IPv6 host address about which to set permit conditions. This <i>destination-ipv6-address</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
dscp <i>value</i>	(Optional) Matches a differentiated services code point (DSCP) value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
authen	(Optional) Matches if the IPv6 authentication header is present.
destopts	(Optional) Matches if the IPv6 destination options header is present.
fragments	(Optional) Matches noninitial fragmented packets where the fragment extension header contains a nonzero fragment offset. The fragments keyword is an option only if the <i>operator</i> [<i>port-number</i>] arguments are not specified.

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 name and sequence number, whether the packet was permitted; 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, and then at 5-minute intervals, including the number of packets permitted in the prior 5-minute interval.
log-input	(Optional) Provides the same function as the log keyword, except that the logging message also includes the input interface.
<i>icmp-type</i>	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<i>icmp-code</i>	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the Acknowledgement (ACK) or Reset (RST) bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
ack	(Optional) For the TCP protocol only: ACK bit set.
fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
psh	(Optional) For the TCP protocol only: Push function bit set.
rst	(Optional) For the TCP protocol only: RST bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.

Defaults

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **permit** (IPv6) command is similar to the **permit** (IPv4) command, except that it is IPv6-specific.

Use the **permit (IPv6)** command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list.

Specifying **ipv6** for the *protocol* argument matches against the IPv6 header of the packet.

By default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 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.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

**Note**

IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator {port | protocol-port}* arguments are not specified.

Examples

The following example configures the IPv6 access list named toCISCO and applies the access list to outbound traffic on packet over SONET (POS) interface 0/2/0/2. Specifically, the first deny entry in the list keeps all packets that have a destination TCP port number greater than 5000 from exiting out of POS interface 0/2/0/2. The second deny entry in the list keeps all packets that have a source UDP port number less than 5000 from exiting out of POS interface 0/2/0/2. The second deny entry also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of POS interface 0/2/0/2. The second permit entry in the list permits all other traffic to exit out of POS interface 0/2/0/2. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list toCISCO

RP/0/RP0/CPU0:router(config-ipv6-acl)# deny tcp any any gt 5000
RP/0/RP0/CPU0:router(config-ipv6-acl)# deny ipv6 any lt 5000 any log
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit icmp any any
RP/0/RP0/CPU0:router(config-ipv6-acl)# permit any any

RP/0/RP0/CPU0:router(config)# interface POS 0/2/0/2
RP/0/RP0/CPU0:router(config-if)# ipv6 access-group toCISCO out
```

Related Commands

Command	Description
deny (IPv6)	Sets deny conditions for an IPv6 access list.
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
remark (IPv6)	Inserts a helpful remark about an IPv6 access list entry.
resequence ipv6 access-list	Changes the starting entry number of the first statement in an existing IPv6 access list, and the number by which subsequent statements are incremented.
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.

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

<i>sequence-number</i>	(Optional) Number of the remark statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
<i>remark</i>	Comment that describes the entry in the access list, up to 255 characters long.

Defaults

The IPv4 access list entries have no remarks.

Command Modes

IPv4 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

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.

Use the **resequence ipv4 access-list** command if you want to add statements to an existing access list and the sequence numbers of consecutive entries does not permit additional statements.

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
```

Related Commands	Command	Description
	deny (IPv4)	Sets conditions under which a packet does not pass a named IPv4 access list.
	ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
	permit (IPv4)	Sets conditions under which a packet passes a named IPv4 access list.
	resequence ipv4 access-list	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.
	show ipv4 access-lists	Displays the contents of all current IPv4 access lists.

remark (IPv6)

To write a helpful comment (remark) for an entry in an IPv6 access list, use the **remark** command in IPv6 access list configuration mode. To remove the remark, use the **no** form of this command.

[sequence-number] **remark** *remark*

no *sequence-number*

Syntax Description

<i>sequence-number</i>	(Optional) Number of the remark statement in the access list. This number determines the order of the statements in the access list. The number can be from 1 to 2147483646. (By default, the first statement is number 10, and the subsequent statements are incremented by 10.)
<i>remark</i>	Comment that describes the entry in the access list, up to 255 characters long.

Defaults

The IPv6 access list entries have no remarks.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **remark** (IPv6) command is similar to the **remark** (IPv4) command, except that it is IPv6-specific.

Use the **remark** command to write a helpful comment for an entry in an IPv6 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.

Use the **resequence ipv6 access-list** command if you want to add statements to an existing access list and the sequence numbers of consecutive entries does not permit additional statements.

Examples

In the following example, a remark is added:

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list Internetfilter
RP/0/RP0/CPU0:router(config-ipv6-acl)# 10 permit ipv6 3333:1:2:3::/64 any
RP/0/RP0/CPU0:router(config-ipv6-acl)# 20 permit ipv6 4444:1:2:3::/64 any
RP/0/RP0/CPU0:router(config-ipv6-acl)# 30 permit ipv6 5555:1:2:3::/64 any
RP/0/RP0/CPU0:router(config-ipv6-acl)# 39 remark Block BGP traffic from a given host
```

```
RP/0/RP0/CPU0:router(config-ipv6-acl)# 40 deny tcp host 6666:1:2:3::10 eq bgp host
7777:1:2:3::20 range 1300 1400
```

```
RP/0/RP0/CPU0:router# show ipv6 access-list Internetfilter
```

```
ipv6 access-list Internetfilter
 10 permit ipv6 3333:1:2:3::/64 any
 20 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
 39 remark Block BGP traffic from a given host
 40 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1400
```

Related Commands

Command	Description
deny (IPv6)	Sets conditions under which a packet does not pass a named IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets conditions under which a packet passes a named IPv6 access list.
resequence ipv6 access-list	Changes the starting entry number of the first statement in an existing IPv6 access list, and the number by which subsequent statements are incremented.
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.

resequence ipv4 access-list

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 ipv4 access-list** command in EXEC mode.

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

Syntax Description

<i>name</i>	Name of an IPv4 access list.
<i>base</i>	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. The maximum value is 2147483646. The default is 10.
<i>increment</i>	(Optional) Number by which the base sequence number is incremented for subsequent statements. The maximum value is 2147483646. The default is 10.

Defaults

base: 10
increment: 10

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **resequence ipv4 access-list** 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 will renumber the existing statements, thereby making room to add new statements with the unused entry numbers.

Examples

In the following 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 ipv4 access-list marketing 20 5
```

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

Related Commands

Command	Description
deny (IPv4)	Sets conditions under which a packet does not pass an IPv4 access list.
ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
permit (IPv4)	Sets conditions under which a packet passes an IPv4 access list.
remark (IPv4)	Adds a remark about an IPv4 access list entry.
show ipv4 access-lists	Displays the contents of all current IPv4 access lists.

resequence ipv6 access-list

To renumber existing statements and increment subsequent statements to allow a new IPv6 access list statement (**permit**, **deny**, or **remark**) to be added, use the **resequence ipv6 access-list** command in EXEC mode.

```
resequence ipv6 access-list name [base [increment]]
```

Syntax Description

<i>name</i>	Name of an IPv6 access list.
<i>base</i>	(Optional) Number of the first statement in the specified access list, which determines its order in the access list. The maximum value is 2147483646. The default is 10.
<i>increment</i>	(Optional) Number by which the base sequence number is incremented for subsequent statements. The maximum value is 2147483646. The default is 10.

Defaults

base: 10
increment: 10

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **resequence ipv6 access-list** command is similar to the **resequence ipv4 access-list** command, except that it is IPv6-specific.

Use the **resequence ipv6 access-list** command to add a **permit**, **deny**, or **remark** statement between consecutive entries in an existing IPv6 access list. Specify the first entry number (the *base*) and the increment by which to separate the entry numbers of the statements. The software will renumber the existing statements, thereby making room to add new statements with the unused entry numbers.

Examples

In the following example, suppose you have an existing access list:

```
ipv6 access-list Internetfilter
 10 permit ipv6 3333:1:2:3::/64 any
 20 permit ipv6 4444:1:2:3::/64 any
 30 permit ipv6 5555:1:2:3::/64 any
```

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 ipv6 access-list Internetfilter 20 5
```

```
RP/0/RP0/CPU0:router# show ipv6 access-list Internetfilter
```

```
ipv6 access-list Internetfilter
```

```
20 permit ipv6 3333:1:2:3::/64 any
25 permit ipv6 4444:1:2:3::/64 any
30 permit ipv6 5555:1:2:3::/64 any
```

Now you add your new entries.

```
RP/0/RP0/CPU0:router(config)# ipv6 access-list Internetfilter
```

```
RP/0/RP0/CPU0:router(config-ipv6-acl)# 3 remark Block BGP traffic from a given host
```

```
RP/0/RP0/CPU0:router(config-ipv6-acl)# 4 deny tcp host 6666:1:2:3::10 eq bgp host
7777:1:2:3::20 range 1300 1400
```

```
RP/0/RP0/CPU0:router# show ipv6 access-list Internetfilter
```

```
ipv6 access-list Internetfilter
```

```
3 remark Block BGP traffic from a given host
4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
20 permit ipv6 3333:1:2:3::/64 any
25 permit ipv6 4444:1:2:3::/64 any
30 permit ipv6 5555:1:2:3::/64 any
```

Related Commands

Command	Description
deny (IPv6)	Sets conditions under which a packet does not pass an IPv6 access list.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets conditions under which a packet passes an IPv6 access list.
remark (IPv6)	Adds a remark about an IPv6 access list entry.
show ipv6 access-lists	Displays the contents of all current IPv6 access lists.

show ipv4 access-lists

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

```
show ipv4 access-lists [access-list-name hardware {ingress | egress} {sequence number | location node-id} | summary [access-list-name] | access-list-name [sequence-number] | oor [detail]]
```

Syntax Description

<i>access-list-name</i>	(Optional) Name of a particular IPv4 access list. The name cannot contain a space or quotation mark; it may contain numbers.
sequence number	(Optional) Sequence number of a particular IPv4 access list. Value is from 1 to 2147483646.
hardware	Identifies the access list as an access list for an interface.
ingress	Specifies an inbound interface.
egress	Specifies an outbound interface.
location <i>node-id</i>	Location of a particular IPv4 access list. The <i>node-id</i> argument is entered in the rack/slot/module notation.
summary	Displays a summary of all current IPv4 access lists.
<i>sequence-number</i>	(Optional) Sequence number of a particular IPv4 access list. Value is from 1 to 2147483646.
oor	Displays the current maximum number of configurable IPv4 ACLs and ACEs.
detail	(Optional) Displays complete out-of-resource (OOR) details.

Defaults

Displays all IPv4 access lists.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

Use the **show ipv4 access-lists** 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** or **egress**, 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 (ingress or egress). 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 ipv4 access-lists 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 ipv4 access-lists oor 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.

Examples

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

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

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
```

In the following example, the contents of an access list named Internetfilter is displayed:

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

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
```

In the following example, the contents of an access list named acl_hw_1 is displayed:

```
RP/0/RP0/CPU0:router# show ipv4 access-lists acl_hw_1 hardware egress location 0/2/cp0

ipv4 access-list acl_hw_1
 10 permit icmp 192.168.36.0 0.0.0.255 any (251 hw matches)
 20 permit ip 172.16.3.0 0.0.255.255 any (29 hw matches)
 30 deny tcp any any (58 hw matches)
```

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

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

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

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

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

Default max configurable acls :5000
Default max configurable aces :200000
Current configured acls      :1
```

■ show ipv4 access-lists

```

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

```

Related Commands	Command	Description
	clear ipv4 access-list	Resets the IPv4 access list match counters.
	copy ipv4 access-list	Copies an existing IPv4 access list.
	deny (IPv4)	Sets conditions under which a packet does not pass a named IPv4 access list.
	ipv4 access-group	Filters incoming or outgoing IPv4 traffic on an interface.
	ipv4 access-list	Defines an IPv4 access list and enters IPv4 access list configuration mode.
	permit (IPv4)	Sets conditions under which a packet passes a named IPv4 access list.
	remark (IPv4)	Inserts a helpful remark about an IPv4 access list entry.
	resequence ipv4 access-list	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.

show ipv6 access-lists

To display the contents of current IPv6 access lists, use the **show ipv6 access-lists** command in EXEC mode.

```
show ipv6 access-lists [access-list-name hardware {ingress | egress} {sequence number |
location node-id} | summary [access-list-name] | access-list-name [sequence-number] | oor
[detail]]
```

Syntax Description		
<i>access-list-name</i>	(Optional) Name of a particular IPv6 access list. The name cannot contain a space or quotation mark; it may contain numbers.	
hardware	Identifies the access list as an access list for an interface.	
ingress	Specifies an inbound interface.	
egress	Specifies an outbound interface.	
location <i>node-id</i>	Location of a particular IPv4 access list. The <i>node-id</i> argument is entered in the rack/slot/module notation.	
sequence number	(Optional) Sequence number of a particular IPv6 access list. Value is from 1 to 2147483646.	
summary	Displays a summary of all current IPv6 access lists.	
<i>sequence-number</i>	(Optional) Sequence number of a particular IPv6 access list. Value is from 1 to 2147483646.	
oor	Displays the current maximum number of configurable IPv6 ACLs and ACEs.	
detail	(Optional) Displays complete out-of-resource (OOR) details.	

Defaults Displays all IPv6 access lists.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, refer to the *Configuring AAA Services on Cisco IOS-XR Software* module of the *Cisco IOS-XR System Security Configuration Guide*.

The **show ipv6 access-lists** command is similar to the **show ipv4 access-lists** command, except that it is IPv6-specific.

Use the **show ipv6 access-lists** command to display the contents of all IPv6 access lists. To display the contents of a specific IPv6 access list, use the *name* argument. Use the *sequence-number* argument to specify the sequence number of the access list.

Use the **hardware**, **ingress** or **egress**, 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 (ingress or egress). 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 **ipv6 access-group** command for access list hardware counters to be enabled.

Use the **show ipv6 access-lists summary** command to display a summary of all current IPv6 access lists. To display a summary of a specific IPv6 access list, use the *name* argument.

Use the **show ipv6 access-lists oor detail** command to display the OOR details for IPv6 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.

Examples

In the following example, the contents of all IPv6 access lists are displayed:

```
RP/0/RP0/CPU0:router# show ipv6 access-lists

ipv6 access-list Internetfilter
 3 remark Block BGP traffic from a given host
 4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
20 permit ipv6 3333:1:2:3::/64 any
25 permit ipv6 4444:1:2:3::/64 any
30 permit ipv6 5555:1:2:3::/64 any
ipv6 access-list marketing
10 permit ipv6 7777:1:2:3::/64 any (51 matches)
20 permit ipv6 8888:1:2:3::/64 any (26 matches)
30 permit ipv6 9999:1:2:3::/64 any (5 matches)
```

In the following example, the contents of an access list named Internetfilter is displayed:

```
RP/0/RP0/CPU0:router# show ipv6 access-lists Internetfilter

ipv6 access-list Internetfilter
 3 remark Block BGP traffic from a given host
 4 deny tcp host 6666:1:2:3::10 eq bgp host 7777:1:2:3::20 range 1300 1404 deny tcp host
171.69.2.88 255.255.0.0 any eq telnet
20 permit ipv6 3333:1:2:3::/64 any
25 permit ipv6 4444:1:2:3::/64 any
30 permit ipv6 5555:1:2:3::/64 any
```

In the following example, the contents of an access list named acl_hw_1 is displayed:

```
RP/0/RP0/CPU0:router# show ipv6 access-lists acl_hw_1 hardware egress location 0/2/cp0

ipv6 access-list acl_hw_1
10 permit icmp any any (251 hw matches)
20 permit ipv6 3333:1:2:3::/64 any (29 hw matches)
30 deny tcp any any (58 hw matches)
```

In the following example, a summary of all IPv6 access lists is displayed:

```
RP/0/RP0/CPU0:router# show ipv6 access-lists summary

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

In the following example, the OOR details of the IPv6 access lists is displayed:

```
RP/0/RP0/CPU0:router# show ipv6 access-list oor detail
Default max configurable acls :1000
```

```

Default max configurable aces :50000
Current configured acls      :1
Current configured aces     :2
Current max configurable acls :1000
Current max configurable aces :50000
Max configurable acls       :2000
Max configurable aces      :100000

```

Related Commands

Command	Description
copy ipv6 access-list	Copies an existing IPv6 access list.
deny (IPv6)	Sets conditions under which a packet does not pass a named IPv6 access list.
ipv6 access-group	Filters incoming or outgoing IPv6 traffic on an interface.
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
permit (IPv6)	Sets conditions under which a packet passes a named IPv6 access list.
remark (IPv6)	Inserts a helpful remark about an IPv4 access list entry.
resequence ipv6 access-list	Changes the starting entry number of the first statement in an existing IPv4 access list, and the number by which subsequent statements are incremented.

■ `show ipv6 access-lists`