

Standard IP Access List Logging

Feature Summary

The Cisco IOS software can now provide logging messages about packets permitted or denied by a standard IP access list. That is, any packet that matches the access list will cause an informational logging message about the packet to be sent to the console. The level of messages logged to the console is controlled by the **logging console** command. This capability was previously only available in extended IP access lists.

The first packet that triggers the access list causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they are displayed or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval.

Benefits

You can monitor how many packets are being permitted or denied by a particular access list, including the source address of each packet.

Platforms

This feature is supported on all platforms.

Configuration Tasks

Perform one of the following tasks to receive logging messages about standard IP access lists. Choose the task you need, depending on whether you are using numbered or named access lists.

- Create a Standard Access List Using Numbers
- Create a Standard Access List Using Names

Regardless of whether you create a numbered or named access list, after you create an access list, you must apply it to either an interface or terminal line for it to be used. That task is described in the section “Apply the Access List to an Interface or Terminal Line” in the chapter “Configuring IP Services” in the *Network Protocols Configuration Guide, Part 1*.

Create a Standard Access List Using Numbers

To create a standard numbered access list and receive logging messages, perform one of the following tasks in global configuration mode:

Task	Command
Define a standard IP access list using a source address and wildcard.	access-list <i>access-list-number</i> {deny permit} <i>source</i> [<i>source-wildcard</i>] log
Define a standard IP access list using an abbreviation for the source and source mask of 0.0.0.0 255.255.255.255.	access-list <i>access-list-number</i> {deny permit} any log

Create a Standard Access List Using Names

To create a standard named access list and receive logging messages, perform the following tasks beginning in global configuration mode:

Task	Command
Step 1 Define a standard IP access list using a name.	ip access-list standard <i>name</i>
Step 2 In access-list configuration mode, specify one or more conditions allowed or denied. This determines whether the packet is passed or dropped.	deny { <i>source</i> [<i>source-wildcard</i>] any } log or permit { <i>source</i> [<i>source-wildcard</i>] any } log
Step 3 Exit access-list configuration mode.	exit

Configuration Example

The following example defines access lists 1 and 2, both of which include logging:

```
interface ethernet 0
 ip address 1.1.1.1 255.0.0.0
 ip access-group 1 in
 ip access-group 2 out
!
access-list 1 permit 5.6.0.0 0.0.255.255 log
access-list 1 deny 7.9.0.0 0.0.255.255 log
!
access-list 2 permit 1.2.3.4 log
access-list 2 deny 1.2.0.0 0.0.255.255 log
```

Suppose the interface receives 10 packets from 5.6.7.7 and 14 packets from 1.2.23.21. The first log will look like this:

```
list 1 permit 5.6.7.7 1 packet
list 2 deny 1.2.23.21 1 packet
```

Five minutes later, the console will receive this log:

```
list 1 permit 5.6.7.7 9 packets
list 2 deny 1.2.23.21 13 packets
```

Command Reference

This section documents the following revised commands for this feature. All other commands used with this feature are documented in the Cisco IOS Release 11.3 command references.

- **access-list (standard)**
- **deny**
- **permit**

access-list (standard)

To define a standard IP access list with a number, use the standard version of the **access-list** global configuration command. To remove a standard access lists, use the **no** form of this command.

```
access-list access-list-number {deny | permit} source [source-wildcard] [log]
no access-list access-list-number
```



Caution Enhancements to this command are backward compatible; migrating from releases prior to Release 10.3 will convert your access lists automatically. However, releases prior to Release 10.3 are not upwardly compatible with these enhancements. Therefore, if you save an access list with these images and then use software prior to Release 10.3, the resulting access list will not be interpreted correctly. **This could cause you severe security problems.** Save your old configuration file before booting these images.

Syntax Description

<i>access-list-number</i>	Number of an access list. This is a decimal number from 1 to 99.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
<i>source</i>	Number of the network or host from which the packet is being sent. There are two 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 keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the <i>source</i> . There are two 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 keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.

log (Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.)

The message includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

Default

The access list defaults to an implicit deny statement for everything. The access list is always terminated by an implicit deny statement for everything.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3. The **log** keyword first appeared in Release 11.3(3)T.

Plan your access conditions carefully and be aware of the implicit deny statement at the end of the access list.

You can use access lists to control the transmission of packets on an interface, control virtual terminal line access, and restrict the contents of routing updates.

Use the **show access-lists EXEC** command to display the contents of all access lists.

Use the **show ip access-list EXEC** command to display the contents of one access list.

Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. The wildcard bits apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.5.34.0 0.0.0.255
access-list 1 permit 128.88.0.0 0.0.255.255
access-list 1 permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the wildcard if it is all zeros. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3 0.0.0.0
```

Related Commands

access-class

access-list (extended)

distribute-list in

distribute-list out

ip access-group

priority-list

queue-list

show access-lists

show ip access-list

deny

To set conditions for a named IP access list, use the **deny** access-list configuration command. To remove a deny condition from an access list, use the **no deny** form of this command.

```
deny { source [source-wildcard] | any } [log]
no deny { source [source-wildcard] | any }

deny protocol source source-wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log]
no deny protocol source source-wildcard destination destination-wildcard
```

For ICMP, you can also use the following syntax:

```
deny icmp source source-wildcard destination destination-wildcard [icmp-type [icmp-code] |
icmp-message] [precedence precedence] [tos tos] [log]
```

For IGMP, you can also use the following syntax:

```
deny igmp source source-wildcard destination destination-wildcard [igmp-type]
[precedence precedence] [tos tos] [log]
```

For TCP, you can also use the following syntax:

```
deny tcp source source-wildcard [operator port [port]] destination destination-wildcard
[operator port [port]] [established] [precedence precedence] [tos tos] [log]
```

For UDP, you can also use the following syntax:

```
deny udp source source-wildcard [operator port [port]] destination destination-wildcard
[operator port [port]] [precedence precedence] [tos tos] [log]
```

Syntax Description

<i>source</i>	Number of the network or host from which the packet is being sent. There are two 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 keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the <i>source</i> . There are two 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 keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords eigrp , gre , icmp , igmp , igrp , ip , ipinip , nos , ospf , tcp , or udp , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip . Some protocols allow further qualifiers described later.

<i>source</i>	<p>Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host source 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>	<p>Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:</p> <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 keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	<p>Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:</p> <ul style="list-style-type: none">• Use a 32-bit quantity in four-part, dotted-decimal format.• Use the keyword any as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host destination 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>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <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 keyword any as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255.• Use host destination 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 name as listed in the section “Usage Guidelines.”</p>
tos <i>tos</i>	<p>(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the “Usage Guidelines” section of the access-list (extended) command.</p>
<i>icmp-type</i>	<p>(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.</p>
<i>icmp-code</i>	<p>(Optional) ICMP packets which are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.</p>

<i>icmp-message</i>	<p>(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the “Usage Guidelines” section of the access-list (extended) command.</p>
<i>igmp-type</i>	<p>(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “Usage Guidelines” section of the access-list (extended) command.</p>
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include 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>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, 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>(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the access-list (extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.</p>
established	<p>(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.</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 for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets.</p> <p>The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers.</p> <p>For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.</p>

Default

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

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2. The **log** keyword for a standard access list first appeared in Release 11.3(3)T.

Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the named access list.

Example

The following example sets a deny condition for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
deny 192.5.34.0 0.0.0.255
permit 128.88.0.0 0.0.255.255
permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip access-group

ip access-list

permit

show ip access-list

permit

To set conditions for a named IP access list, use the **permit** access-list configuration command. To remove a condition from an access list, use the **no permit** form of this command.

```
permit {source [source-wildcard] | any} [log]  
no permit {source [source-wildcard] | any}
```

```
permit protocol source source-wildcard destination destination-wildcard [precedence  
precedence] [tos tos] [log]  
no permit protocol source source-wildcard destination destination-wildcard [precedence  
precedence] [tos tos] [log]
```

For ICMP, you can also use the following syntax:

```
permit icmp source source-wildcard destination destination-wildcard [icmp-type [icmp-code] |  
icmp-message] [precedence precedence] [tos tos] [log]
```

For IGMP, you can also use the following syntax:

```
permit igmp source source-wildcard destination destination-wildcard [igmp-type]  
[precedence precedence] [tos tos] [log]
```

For TCP, you can also use the following syntax:

```
permit tcp source source-wildcard [operator port [port]] destination destination-wildcard  
[operator port [port]] [established] [precedence precedence] [tos tos] [log]
```

For UDP, you can also use the following syntax:

```
permit udp source source-wildcard [operator port [port]] destination destination-wildcard  
[operator port [port]] [precedence precedence] [tos tos] [log]
```

Syntax Description

<i>source</i>	Number of the network or host from which the packet is being sent. There are two 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 keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>source-wildcard</i>	(Optional) Wildcard bits to be applied to the <i>source</i> . There are two 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 keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255.
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords eigrp , gre , icmp , igmp , igrp , ip , ipinip , nos , ospf , tcp , or udp , or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the keyword ip . Some protocols allow further qualifiers described later.

<i>source</i>	<p>Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source 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>	<p>Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:</p> <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 keyword any as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host source as an abbreviation for a <i>source</i> and <i>source-wildcard</i> of <i>source</i> 0.0.0.0.
<i>destination</i>	<p>Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:</p> <ul style="list-style-type: none"> • Use a 32-bit quantity in four-part, dotted-decimal format. • Use the keyword any as an abbreviation for the <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination 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>	<p>Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:</p> <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 keyword any as an abbreviation for a <i>destination</i> and <i>destination-wildcard</i> of 0.0.0.0 255.255.255.255. • Use host destination 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 name as listed in the section “Usage Guidelines.”</p>
tos <i>tos</i>	<p>(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the “Usage Guidelines” section of the access-list (extended) command.</p>
<i>icmp-type</i>	<p>(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.</p>
<i>icmp-code</i>	<p>(Optional) ICMP packets which are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.</p>

<i>icmp-message</i>	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the “Usage Guidelines” section of the access-list (extended) command.
<i>igmp-type</i>	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “Usage Guidelines” section of the access-list (extended) command.
<i>operator</i>	<p>(Optional) Compares source or destination ports. Possible operands include 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>, it must match the source port.</p> <p>If the operator is positioned after the <i>destination</i> and <i>destination-wildcard</i>, 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>	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the access-list (extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
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 for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets.</p> <p>The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers.</p> <p>For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.</p>

Default

There are no specific conditions under which a packet passes the named access list.

Command Mode

Access-list configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2. The **log** keyword for a standard access list first appeared in Release 11.3(3)T.

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

Example

The following example sets conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
deny 192.5.34.0 0.0.0.255
permit 128.88.0.0 0.0.255.255
permit 36.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
```

Related Commands

deny

ip access-group

ip access-list

show ip access-list

