

IP Access List Configuration Commands

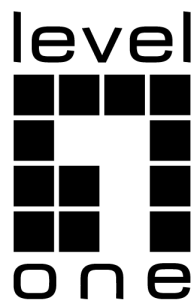


Table of Contents

Chapter 1 Configuring IP Access List Commands.....	1
1.1 IP Access List Configuration Commands	1
1.1.1 deny	1
1.1.2 ip access-list.....	3
1.1.3 permit	4
1.1.4 show ip access-list	6

Chapter 1 Configuring IP Access List Commands

1.1 IP Access List Configuration Commands

- deny
- ip access-list
- permit
- show ip access-list

1.1.1 deny

Syntax

To set conditions in a named IP access list that will deny packets, use the deny command in access list configuration mode. To remove a deny condition from an access list, use the no form of this command.

deny source [*source-mask*]

no deny source [*source-mask*]

deny protocol source source-mask destination destination-mask [**tos** tos]

no deny protocol source source-mask destination destination-mask [**tos** tos]

For the Internet Control Message Protocol (ICMP), the following syntax can also be used:

deny icmp source source-mask destination destination-mask [*icmp-type*] [**tos** tos]

For the Internet Group Management Protocol (IGMP), the following syntax can also be used:

deny igmp source source-mask destination destination-mask [*igmp-type*] [**tos** tos]

For the Transmission Control Protocol (TCP), the following syntax can also be used:

deny tcp source source-mask [*operator port*] **destination destination-mask** [*operator port*] [**tos** tos]

For the User Datagram Protocol (UDP), the following syntax can also be used:

deny udp source source-mask [*operator port*] **destination destination-mask** [*operator port*] [**tos** tos]

Parameter

parameter	Description
<i>protocol</i>	Name or number of an Internet protocol. The protocol argument can be one of the keywords icmp, igmp, igmp, ip, ospf, tcp or udp, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP and UDP), use the keyword ip. Some protocols allow for further restrictions, as described below.
<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. Use a 32-bit quantity in four-part dotted-decimal format. Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 0.0.0.0.

<i>source-mask</i>	Source address network mask. Use the any keyword as an abbreviation for the source mask and source of 0.0.0.0 0.0.0.
<i>destination</i>	Number of the network or host to which the packet is being sent. There are two alternative ways to specify the destination: Use a 32-bit quantity in four-part dotted-decimal format. Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 255.255.255.255.
<i>destination-mask</i>	Destination address network mask. Use the any keyword as an abbreviation for the destination address and destination address mask of 0.0.0.0 0.0.0.
tos tos	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15.
<i>icmp-type</i>	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
<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.
<i>operator</i>	(Optional) Compares source or destination ports. Operators include eq (equal). If the operator is positioned after the source and source-wildcard arguments, it must match the source port. If the operator is positioned after the destination and destination-wildcard arguments, it must match the destination port.
<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.

Command mode

IP Access List Configuration Mode

Usage Guidelines

You can use the access list to control the transmission of packets on the interface, control virtual terminal line access, and limit the content of routing updates. Stop checking the extended access list after the match occurs. Fragmented IP packets, rather than initial segments, are immediately received by any extended IP access table. The extended access table is used to control access to virtual terminal lines or restrict the content of routing updates, without matching the TCP source port, the type of service value, or the priority of the packet.

Note:

After initially establishing an access list, any subsequent adding content (which can be input by terminal) is put in the bottom of the list.

Example

The following example denies the network range 192.168.5.0:

```
Switch(config)#ip access-list standard filter
Switch(config-filter)#deny 192.168.5.0 255.255.255.0
```

Note:

IP access table is concluded in a cryptic deny rule.

Related commands

ip access-group
ip access-list
permit
show ip access-list

1.1.2 ip access-list**Syntax**

To define an IP access list by name or number, use the `ip access-list` command in global configuration mode. To remove the IP access list, use the `no` form of this command.

ip access-list {standard | extended} *name*
no ip access-list {standard | extended} *name*

Parameter

parameter	description
standard	Specifies a standard IP access list.
extended	Specifies an extended IP access list.
<i>name</i>	Name of the access list. The string of up to 20 characters.

Default

No IP access list is defined.

Command mode

Global configuration mode

Usage Guidelines

Use this command to configure a named or numbered IP access list. This command will place the switch in access-list configuration mode, where you must define the denied or permitted access conditions with the `deny` and `permit` commands.

Example

The following example defines a standard access list:

```
Switch(config)#ip access-list standard filter
Switch(config-filter)#deny 192.168.1.0 255.255.255.0
Switch(config-filter)#permit any
```

Related commands

deny
ip access-group

permit**show ip access-list**

1.1.3 permit

Syntax

To set conditions to allow a packet to pass a named IP access list, use the permit command in access list configuration mode. To remove a permit condition from an access list, use the no form of this command.

permit source *[source-mask]*

no permit source *[source-mask]*

permit protocol source *source-mask destination destination-mask [tos tos]*

no permit protocol source *source-mask destination destination-mask [tos tos]*

Internet Control Message Protocol (ICMP)

permit icmp source *source-mask destination destination-mask [icmp-type] [tos tos]*

Internet Group Management Protocol (IGMP)

permit igmp source *source-mask destination destination-mask [igmp-type] [tos tos]*

Transmission Control Protocol (TCP)

permit tcp source *source-mask [operator port] destination destination-mask [operator port] [tos tos]*

User Datagram Protocol (UDP)

permit udp source *source-mask [operator port [port]] destination destination-mask [operator port [port]] [tos tos]*

Parameter

parameter	Description
<i>protocol</i>	Name or number of an Internet protocol. The protocol argument can be one of the keywords icmp, igmp, igmp, ip, ospf, tcp or udp, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP and UDP), use the keyword ip. Some protocols allow for further restrictions, as described below.
<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. Use a 32-bit quantity in four-part dotted-decimal format. Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 0.0.0.0.
<i>source-mask</i>	Source address network mask. Use the any keyword as an abbreviation for the source mask and source of 0.0.0.0 0.0.0.0.
<i>destination</i>	Number of the network or host to which the packet is being sent. There are two alternative ways to specify the destination: Use a 32-bit quantity in four-part dotted-decimal format. Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 255.255.255.255.
<i>destination-mask</i>	Destination address network mask. Use the any keyword as an abbreviation for the destination address and destination address mask of 0.0.0.0 0.0.0.0.

tos <i>tos</i>	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15.
operator	(Optional) Compares source or destination ports. Operators include eq (equal). If the operator is positioned after the source and source-wildcard arguments, it must match the source port. If the operator is positioned after the destination and destination-wildcard arguments, it must match the destination port.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535.

Command mode

IP access list configuration

Usage Guidelines

You can use the access list to control the transmission of packets on the interface, control virtual terminal line access, and limit the content of routing updates. Stop checking the extended access list after the match occurs. Fragmented IP packets, rather than initial segments, are immediately received by any extended IP access table. The extended access table is used to control access to virtual terminal lines or restrict the content of routing updates, without matching the TCP source port, the type of service value, or the priority of the packet.

Note:

After initially establishing an access list, any subsequent adding content (which can be input by terminal) is put in the bottom of the list.

Example

The following example permits network range 192.168.5.0:

```
Switch(config)#ip access-list standard filter
Switch(config-filter)#permit 192.168.5.0 255.255.255.0
```

Note:

IP access table is concluded in a cryptic deny rule.

Related commands

deny

ip access-group

ip access-list

show ip access-list

1.1.4 show ip access-list

Syntax

To display the contents of all current IP access lists, use the `show ip access-list` command.

show ip access-list*[access-list-name]*

Parameter

parameter	Description
<i>access-list-name</i>	Name of the IP access list to display. The string of up to 20 characters.

Default

All standard and extended IP access lists are displayed.

Command mode

EXEC

Usage Guidelines

The `show ip access-list` command provides output identical to the `show access-lists` command, except that it is IP-specific and allows you to specify a particular access list

Example

The following is sample output from the **show ip access-list** command when the name of a specific access list is not requested:

```
Switch#show ip access-list
Standard IP access list test1
  Index      Rule content
-----
      1      permit 10.1.1.2 255.255.255.255
      2      deny    any
Extended IP access list test2
  Index      Rule content
-----
      1      deny    ip interface VLAN4 any time-range time1
      2      deny    icmp interface VLAN4 any time-range time2
      3      permit  icmp interface VLAN4 any time-range time3
```

The following is sample output from the **show ip access-list** command when the name of a specific access list is requested:

```
Switch#show ip access-list test1
Standard IP access list test1
  Index      Rule content
-----
      1      permit 10.1.1.2 255.255.255.255
      2      deny    any
```