# IP Access List Configuration Commands

# Table of Contents

Chapter 1 Configuring Physical Interface IP Access List Command ..... 1
1.1 IP Access List Configuration Commands Based on Physical Interface ..... 1
1.1.1 deny ..... 1
1.1.2 ip access-group ..... 3
1.1.3 ip access-list ..... 4
1.1.4 permit ..... 5
1.1.5 show ip access-list ..... 7

# Chapter 1 Configuring Physical Interface IP Access List Command

## 1.1 IP Access List Configuration Commands Based on Physical Interface

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

### 1.1.1 deny

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]

Internet Control Message Protocol (ICMP)

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

Internet Group Management Protocol (IGMP)

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

Transmission Control Protocol (TCP)

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

User Datagram Protocol (UDP)

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

parameter

| parameter | Description |
|---|---|
| *protocol* | Name or number of an Internet protocol. The protocol argument can be one of the keywords eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, or udp, or an integer in the range from 0 to 255 representing an Internet protocol number. |
| source | 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. |
| *source-mask* | Source address network masn. Use the any keyword as an abbreviation for the source mask and source of 0.0.0.0 0.0.0. |
| *destination* | Number of the network or host to which the packet is being sent. There are two alternative ways to specify the destination:<br>Use a 32-bit quantity in four-part dotted-decimal format.<br>Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 255.255.255.255. |
| destination-mask | 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, or by a name as listed in the "Usage Guidelines" section of the access-list (IP extended) command. |
| 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. IGMP message names are listed in the "Usage Guidelines" section of the access-list (IP extended) command. |
| operator | (Optional) Compares source or destination ports. Operators include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).<br>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 Mode

## Instruction

Use this command following the ip access-list command to specify conditions under which a packet cannot pass the named access list. The time-range keyword allows you to identify a time range by name. The time-range, absolute, and periodic commands specify when this deny statement is in effect.

**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:

ip access-list standard filter
deny 192.168.5.0 255.255.255.0

**Note:**

IP access table is concluded in a crytic deny rule.

### Related commands

**ip access-group**

**ip access-list**

**permit**

**show ip access-list**

## 1.1.2 ip access-group

To apply an access control list to control packet access, use the ip access-group command in the appropriate configuration mode. To remove the specified access group, use the no form of this command.

**ip access-group** {*access-list-name*}

**no ip access-group** {*access-list-name*}

### parameter

| parameter | Description |
|---|---|
| *access-list-name* | Name of an IP access list as specified by an ip access-list command. |

### Command mode

Interface configuration mode

### Instruction

Access lists can be applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message. If the specified access list does not exist, all packets are passed.

### example

The following example applies list  on packets outbound from Ethernet interface g0/10::

```
Interface g0/10
ip access-group filter
```

related commands

**ip access-list**

**show ip access-list**

### 1.1.3 ip access-list

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. |
| *name* | Name of the access list. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists. |

default

No IP access list is defined.

Command mode

**global configuration mode**

instruction

Use this command to configure a named or numbered IP access list. This command will place the router 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:

```
ip access-list standard filter
deny 192.168.1.0 255.255.255.0
permit any
```

related commands

**deny**

**ip access-group**

**permit**

**show ip access-list**

## 1.1.4 permit

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* [**tos** *tos*]

### parameter

| parameter | description |
|---|---|
| **protocol** | Name or number of an Internet protocol. The protocol argument can be one of the keywords eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, or udp, or an integer in the range from 0 to 255 representing an Internet protocol number. |
| **source** | 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. |
| *source-mask* | Source address network masn. Use the any keyword as an abbreviation for the source mask and source of 0.0.0.0 0.0.0. |
| **destination** | Number of the network or host to which the packet is being sent. There are two alternative ways to specify the destination:<br>Use a 32-bit quantity in four-part dotted-decimal format.<br>Use the any keyword as an abbreviation for the destination and destination-wildcard of 0.0.0.0 255.255.255.255. |
| *destination-mask* | 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, or by a name as listed in the "Usage Guidelines" section of the access-list (IP extended) command. |
| 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. IGMP message names are listed in the "Usage Guidelines" section of the access-list (IP extended) command. |
| **operator** | (Optional) Compares source or destination ports. Operators include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).<br><br>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

Access list configuration

## Instruction

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

The time-range keyword allows you to identify a time range by name. The time-range, absolute, and periodic commands specify when this permit statement is in effect.

**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:

ip access-list standard filter
permit 192.168.5.0 255.255.255.0

**Note:**

IP access table is concluded in a crytic deny rule.

## Related commands

**deny**

**ip access-group**

**ip access-list**

**show ip access-list**

### 1.1.5 show ip access-list

To display the contents of all current IP access lists, use the show ip access-list command in user EXEC or privileged EXEC mode.

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

#### parameter

| parameter | Description |
|---|---|
| *access-list-name* | Name of the IP access list to display. |

#### default

All standard and extended IP access lists are displayed.

#### Command mode

EXEC

#### Instruction

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
ip access-list standard aaa
permit 192.2.2.1
permit 192.3.3.0 255.255.255.0
ip access-list extended bbb
permit tcp any any eq 25
permit ip any any
```

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

```
ip access-list extended bbb
permit tcp any any eq 25
permit ip any any
```