# P Commands

This chapter describes the Cisco NX-OS security commands that begin with P.

# permit (ARP)

To create an ARP ACL rule that permits ARP traffic that matches its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

**General Syntax**

[*sequence-number*] **permit ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

**no** *sequence-number*

**no permit ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

| Syntax Description | | |
|---|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. | |
| | A sequence number can be any integer between 1 and 4294967295. | |
| | By default, the first rule in an ACL has a sequence number of 10. | |
| | If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. | |
| | Use the **resequence** command to reassign sequence numbers to rules. | |
| **ip** | Introduces the IP address portion of the rule. | |
| **any** | Specifies that any host matches the part of the rule that contains the **any** keyword. You can use **any** to specify the sender IP address, target IP address, sender MAC address, and target MAC address. | |
| **host** *sender-IP* | Specifies that the rules matches ARP packets only when the sender IP address in the packet matches the value of the *sender-IP* argument. Valid values for the *sender-IP* argument are IPv4 addresses in dotted-decimal format. | |
| *sender-IP sender-IP-mask* | IPv4 address and mask for the set of IPv4 addresses that the sender IP address in the packet can match. The *sender-IP* and *sender-IP-mask* argument must be in dotted-decimal format. Specifying 255.255.255.255 as the *sender-IP-mask* argument is the equivalent of using the **host** keyword. | |
| **mac** | Introduces the MAC address portion of the rule. | |

**Command Default**   None

**Command Modes**   ARP ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    A newly created ARP ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

When the device applies an ARP ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

**Examples**    This example shows how to enter ARP access list configuration mode for an ARP ACL named copp-arp-acl and add a rule that permits ARP request messages that contain a sender IP address that is within the 192.0.32.14/24 subnet and associate them with the copp-arp-acl class:

```
switch# configure terminal
switch(config)# arp access-list copp-arp-acl
switch(config-arp-acl)# permit ip 192.0.32.14 255.255.255.0 mac any
switch(config-arp-acl)#
```

**Related Commands**

| Command | Description |
| --- | --- |
| deny (ARP) | Configures a deny rule in an ARP ACL. |
| arp access-list | Configures an ARP ACL. |
| remark | Configures a remark in an ACL. |
| show arp access-lists | Displays all ARP ACLs or one ARP ACL. |

# permit icmp (IPv4)

To create an access control list (ACL) rule that permits IPv4 ICMP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

Need to test this: *sequence-number*] **permit icmp** *source destination* [*icmp-message*]

[*sequence-number*] **permit icmp** *source destination* [*icmp-message* | **dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

**no permit icmp** *source destination* [*icmp-message* | **dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

**no** *sequence-number*

> **Note**    You can also specify the **icmp** keyword by its protocol number. Valid numbers are from 0 to 255.

| Syntax Descriptionl | | |
|---|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. | |
| | A sequence number can be any integer between 1 and 4294967295. | |
| | By default, the first rule in an ACL has a sequence number of 10. | |
| | If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. | |
| | Use the **resequence** command to reassign sequence numbers to rules. | |
| *source* | Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "iSource and Destination" section in the "Usage Guidelines" section. | |
| *destination* | Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "iSource and Destination" section in the "Usage Guidelines" section. | |
| icmp-message | ICMP message number, which is an integer from 0 to 255, or a keyword. For a list of keywords, see the "ICMP Message Types" section in the "Usage Guidelines" section. | |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **fragments** | (Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments. |

| | |
|---|---|
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |
| | • Protocol |
| | • Source and destination addresses |
| | • Source and destination port numbers, if applicable |
| **precedence** *precedence* | (Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: |
| | • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. |
| | • **critical**—Precedence 5 (101) |
| | • **flash**—Precedence 3 (011) |
| | • **flash-override**—Precedence 4 (100) |
| | • **immediate**—Precedence 2 (010) |
| | • **internet**—Precedence 6 (110) |
| | • **network**—Precedence 7 (111) |
| | • **priority**—Precedence 1 (001) |
| | • **routine**—Precedence 0 (000) |

**Command Default**  A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

**Command Modes**  IPv4 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**  When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

**iSource and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address network-wildcard*

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit icmp 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit icmp 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  ```
  switch(config-acl)# permit icmp host 192.168.67.132 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

### ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **administrativelyprohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply
- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS

- **host-unknown**—Host unknown

- **host-unreachable**—Host unreachable

- **information-reply**—Information replies

- **information-request**—Information requests

- **log**—Log matches against this entry

- **mask-reply**—Mask replies

- **mask-request**—Mask requests

- **mobile-redirect**—Mobile host redirect

- **net-redirect**—Network redirect

- **net-tos-redirect**—Net redirect for ToS

- **net-tos-unreachable**—Network unreachable for ToS

- **net-unreachable**—Net unreachable

- **network-unknown**—Network unknown

- **no-room-for-option**—Parameter required but no room

- **option-missing**—Parameter required but not present

- **packet-too-big**—Fragmentation needed and DF set

- **parameter-problem**—All parameter problems

- **port-unreachable**—Port unreachable

- **precedence-unreachable**—Precedence cutoff

- **protocol-unreachable**—Protocol unreachable

- **reassembly-timeout**—Reassembly timeout

- **redirect**—All redirects

- **router-advertisement**—Router discovery advertisements

- **router-solicitation**—Router discovery solicitations

- **source-quench**—Source quenches

- **source-route-failed**—Source route failed

- **time-exceeded**—All time-exceeded messages

- **timestamp-reply**—Time-stamp replies

- **timestamp-request**—Time-stamp requests

- **traceroute**—Traceroute

- **ttl-exceeded**—TTL exceeded

- **unreachable**—All unreachables

**Examples**        This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all ICMP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
switch(config)# ip access-list acl-lab-01
switch(config)# permit icmp 10.23.0.0/16 10.176.0.0/16
switch(config)# permit icmp 192.168.37.0/16 10/176.0.0/16
```

| Related Commands | Command | Description |
|---|---|---|
| | **deny (IPv4)** | Configures a deny rule in an IPv4 ACL. |
| | **ip access-list** | Configures an IPv4 ACL. |
| | **remark** | Configures a remark in an ACL. |
| | **show ip access-lists** | Displays all IPv4 ACLs or one IPv4 ACL. |

# permit igmp (IPv4)

To create an access control list (ACL) rule that permits IPv4 IGMP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **permit igmp** *source destination* [*igmp-message* | **dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

**no permit igmp** *source destination* [*igmp-message* | **dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

**no** *sequence-number*

---

✎ **Note**    You can also specify the **igmp** keyword by its protocol number. Valid numbers are from 0 to 255.

---

| Syntax Description | | |
|---|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. | |
| | A sequence number can be any integer between 1 and 4294967295. | |
| | By default, the first rule in an ACL has a sequence number of 10. | |
| | If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. | |
| | Use the **resequence** command to reassign sequence numbers to rules. | |
| **igmp** | Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-message* argument is available. | |
| *source* | Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. | |
| *destination* | Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" in the "Usage Guidelines" section. | |
| *igmp-message* | (Optional) Rule that matches only packets of the specified IGMP message type. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords:<br><br>• **dvmrp**—Distance Vector Multicast Routing Protocol<br>• **host-query**—Host query<br>• **host-report**—Host report<br>• **log**—Log matches against this entry<br>• **pim**—Protocol Independent Multicast<br>• **trace**—Multicast trace | |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **fragments** | (Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments. |

| log | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |
|---|---|
| | • Protocol |
| | • Source and destination addresses |
| | • Source and destination port numbers, if applicable |
| **precedence** *precedence* | (Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: |
| | • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. |
| | • **critical**—Precedence 5 (101) |
| | • **flash**—Precedence 3 (011) |
| | • **flash-override**—Precedence 4 (100) |
| | • **immediate**—Precedence 2 (010) |
| | • **internet**—Precedence 6 (110) |
| | • **network**—Precedence 7 (111) |
| | • **priority**—Precedence 1 (001) |
| | • **routine**—Precedence 0 (000) |

**Command Default**  A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

**Command Modes**  IPv4 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**  When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address network-wildcard*

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit igmp 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit igmp 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  ```
  switch(config-acl)# permit igmp host 192.168.67.132 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

**Examples**    This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all IGMP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit igmp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit igmp 192.168.37.0/16 10.176.0.0/16
```

**Related Commands**

| Command | Description |
|---|---|
| **deny (IPv4)** | Configures a deny rule in an IPv4 ACL. |
| **ip access-list** | Configures an IPv4 ACL. |
| **remark** | Configures a remark in an ACL. |
| **show ip access-lists** | Displays all IPv4 ACLs or one IPv4 ACL. |

# permit ip (IPv4)

To create an access control list (ACL) rule that permits IPv4 traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **permit ip** *source destination* [ **dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

**no permit ip** *source destination* [ **dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

**no** *sequence-number*

| Syntax Description | | |
|---|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. | |
| | A sequence number can be any integer between 1 and 4294967295. | |
| | By default, the first rule in an ACL has a sequence number of 10. | |
| | If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. | |
| | Use the **resequence** command to reassign sequence numbers to rules. | |
| *source* | Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. | |
| *destination* | Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section. | |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **fragments** | (Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments. |

| | |
|---|---|
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |
| | • Protocol |
| | • Source and destination addresses |
| | • Source and destination port numbers, if applicable |
| **precedence** *precedence* | (Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: |
| | • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. |
| | • **critical**—Precedence 5 (101) |
| | • **flash**—Precedence 3 (011) |
| | • **flash-override**—Precedence 4 (100) |
| | • **immediate**—Precedence 2 (010) |
| | • **internet**—Precedence 6 (110) |
| | • **network**—Precedence 7 (111) |
| | • **priority**—Precedence 1 (001) |
| | • **routine**—Precedence 0 (000) |

**Command Default**     A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

**Command Modes**     IPv4 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**     When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address network-wildcard*

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit ip 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  switch(config-acl)# permit ip 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  ```
  switch(config-acl)# permit ip host 192.168.67.132 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

**Examples**

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit ip 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit ip 192.168.37.0/16 10.176.0.0/16
```

**Related Commands**

| Command | Description |
| --- | --- |
| **deny (IPv4)** | Configures a deny rule in an IPv4 ACL. |
| **ip access-list** | Configures an IPv4 ACL. |
| **remark** | Configures a remark in an ACL. |
| **show ip access-lists** | Displays all IPv4 ACLs or one IPv4 ACL. |

# permit tcp (IPv4)

To create an access control list (ACL) rule that permits IPv4 TCP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **fragments** | **log** | **precedence** *precedence* | *flags* | **established**]

**no permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **fragments** | **log** | **precedence** *precedence* | *flags* | **established**]

**no** *sequence-number*

**Syntax Description**

| | |
|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL.<br><br>A sequence number can be any integer between 1 and 4294967295.<br><br>By default, the first rule in an ACL has a sequence number of 10.<br><br>If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule.<br><br>Use the **resequence** command to reassign sequence numbers to rules. |
| *source* | Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |
| *destination* | Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |

| | |
|---|---|
| *operator port* [*port*] | (Optional) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. |
| | The *port* argument can be the name or the number of a TCP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the "TCP Port Names" section in the "Usage Guidelines" section. |
| | A second *port* argument is required only when the *operator* argument is a range. |
| | The *operator* argument must be one of the following keywords: |
| | • **eq**—Matches only if the port in the packet is equal to the *port* argument. |
| | • **gt**—Matches only if the port in the packet is greater than the *port* argument. |
| | • **lt**—Matches only if the port in the packet is less than the *port* argument. |
| | • **neq**—Matches only if the port in the packet is not equal to the *port* argument. |
| | • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument. |
| **portgroup** *portgroup* | (Optional) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. |
| | Use the **object-group ip port** command to create and change IP port-group objects. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **fragments** | (Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments. |
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |
| | • Protocol |
| | • Source and destination addresses |
| | • Source and destination port numbers, if applicable |

| | |
|---|---|
| **precedence** *precedence* | (Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: |

- 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011.

- **critical**—Precedence 5 (101)

- **flash**—Precedence 3 (011)

- **flash-override**—Precedence 4 (100)

- **immediate**—Precedence 2 (010)

- **internet**—Precedence 6 (110)

- **network**—Precedence 7 (111)

- **priority**—Precedence 1 (001)

- **routine**—Precedence 0 (000)

| | |
|---|---|
| *flags* | (Optional) Rule that matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: |

- **ack**

- **fin**

- **psh**

- **rst**

- **syn**

- **urg**

| | |
|---|---|
| **established** | (Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The switch considers TCP packets with the ACK or RST bits set to belong to an established connection. |

**Command Default**   A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

**Command Modes**   IPv4 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**   When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address network-wildcard*

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  switch(config-acl)# **permit tcp 192.168.67.0 0.0.0.255 any**

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  switch(config-acl)# **permit tcp 192.168.67.0/24 any**

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  switch(config-acl)# **permit tcp host 192.168.67.132 any**

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

**TCP Port Names**

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **bgp**—Border Gateway Protocol (179)
- **chargen**—Character generator (19)
- **cmd**—Remote commands (rcmd, 514)
- **daytime**—Daytime (13)
- **discard**—Discard (9)
- **domain**—Domain Name Service (53)
- **drip**—Dynamic Routing Information Protocol (3949)
- **echo**—Echo (7)
- **exec**—EXEC (rsh, 512)
- **finger**—Finger (79)

- **ftp**—File Transfer Protocol (21)
- **ftp-data**—FTP data connections (2)
- **gopher**—Gopher (7)
- **hostname**—NIC hostname server (11)
- **ident**—Ident Protocol (113)
- **irc**—Internet Relay Chat (194)
- **klogin**—Kerberos login (543)
- **kshell**—Kerberos shell (544)
- **login**—Login (rlogin, 513)
- **lpd**—Printer service (515)
- **nntp**—Network News Transport Protocol (119)
- **pim-auto-rp**—PIM Auto-RP (496)
- **pop2**—Post Office Protocol v2 (19)
- **pop3**—Post Office Protocol v3 (11)
- **smtp**—Simple Mail Transport Protocol (25)
- **sunrpc**—Sun Remote Procedure Call (111)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **telnet**—Telnet (23)
- **time**—Time (37)
- **uucp**—Unix-to-Unix Copy Program (54)
- **whois**—WHOIS/NICNAME (43)
- **www**—World Wide Web (HTTP, 8)

**Examples**

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit tcp 192.168.37.0/16 10.176.0.0/16
```

**Related Commands**

| Command | Description |
|---------|-------------|
| **deny (IPv4)** | Configures a deny rule in an IPv4 ACL. |
| **ip access-list** | Configures an IPv4 ACL. |
| **remark** | Configures a remark in an ACL. |
| **show ip access-lists** | Displays all IPv4 ACLs or one IPv4 ACL. |

# permit udp (IPv4)

To create an access control list (ACL) rule that permits IPv4 UDP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

**General Syntax**

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

**no permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **fragments** | **log** | **precedence** *precedence*]

**no** *sequence-number*

**Syntax Descriptionl**

| | |
|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. |
| | A sequence number can be any integer between 1 and 4294967295. |
| | By default, the first rule in an ACL has a sequence number of 10. |
| | If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. |
| | Use the **resequence** command to reassign sequence numbers to rules. |
| *source* | Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |
| *destination* | Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |

| | |
|---|---|
| *operator port* [*port*] | (Optional) Rule that matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument.<br><br>The *port* argument can be the name or the number of a UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the "UDP Port Names" section in the "Usage Guidelines" section.<br><br>A second *port* argument is required only when the *operator* argument is a range.<br><br>The *operator* argument must be one of the following keywords:<br><br>• **eq**—Matches only if the port in the packet is equal to the *port* argument.<br><br>• **gt**—Matches only if the port in the packet is greater than the *port* argument.<br><br>• **lt**—Matches only if the port in the packet is less than the *port* argument.<br><br>• **neq**—Matches only if the port in the packet is not equal to the *port* argument.<br><br>• **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument. |
| **portgroup** *portgroup* | (Optional) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument.<br><br>Use the **object-group ip port** command to create and change IP port-group objects. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **fragments** | (Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the switch requires to evaluate those options is contained only in initial fragments. |

| | |
|---|---|
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |
| | • Protocol |
| | • Source and destination addresses |
| | • Source and destination port numbers, if applicable |
| **precedence** *precedence* | (Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword as follows: |
| | • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. |
| | • **critical**—Precedence 5 (101) |
| | • **flash**—Precedence 3 (011) |
| | • **flash-override**—Precedence 4 (100) |
| | • **immediate**—Precedence 2 (010) |
| | • **internet**—Precedence 6 (110) |
| | • **network**—Precedence 7 (111) |
| | • **priority**—Precedence 1 (001) |
| | • **routine**—Precedence 0 (000) |

**Command Default**   A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

**Command Modes**   IPv4 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**   When the switch applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address network-wildcard*

  This example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  switch(config-acl)# **permit udp 192.168.67.0 0.0.0.255 any**

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  switch(config-acl)# **permit udp 192.168.67.0/24 any**

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  This example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  switch(config-acl)# **permit udp host 192.168.67.132 any**

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

### UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **biff**—Biff (mail notification, comsat, 512)
- **bootpc**—Bootstrap Protocol (BOOTP) client (68)
- **bootps**—Bootstrap Protocol (BOOTP) server (67)
- **discard**—Discard (9)
- **dnsix**—DNSIX security protocol auditing (195)
- **domain**—Domain Name Service (DNS, 53)
- **echo**—Echo (7)
- **isakmp**—Internet Security Association and Key Management Protocol (5)
- **mobile-ip**—Mobile IP registration (434)
- **nameserver**—IEN116 name service (obsolete, 42)
- **netbios-dgm**—NetBIOS datagram service (138)
- **netbios-ns**—NetBIOS name service (137)
- **netbios-ss**—NetBIOS session service (139)

- **non500-isakmp**—Internet Security Association and Key Management Protocol (45)
- **ntp**—Network Time Protocol (123)
- **pim-auto-rp**—PIM Auto-RP (496)
- **rip**—Routing Information Protocol (router, in.routed, 52)
- **snmp**—Simple Network Management Protocol (161)
- **snmptrap**—SNMP Traps (162)
- **sunrpc**—Sun Remote Procedure Call (111)
- **syslog**—System Logger (514)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **tftp**—Trivial File Transfer Protocol (69)
- **time**—Time (37)
- **who**—Who service (rwho, 513)
- **xdmcp**—X Display Manager Control Protocol (177)

**Examples**    This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit udp 192.168.37.0/16 10.176.0.0/16
```

**Related Commands**

| Command | Description |
| --- | --- |
| **deny (IPv4)** | Configures a deny rule in an IPv4 ACL. |
| **ip access-list** | Configures an IPv4 ACL. |
| **remark** | Configures a remark in an ACL. |
| **show ip access-lists** | Displays all IPv4 ACLs or one IPv4 ACL. |

# permit icmp (IPv6)

To create an access control list (ACL) rule that permits IPv6 ICMP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

**General Syntax**

[*sequence-number*] **permit icmp** *source destination* [*icmp-message* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

**no permit permit icmp** *source destination* [*icmp-message* | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

**no** *sequence-number*

| Syntax Description | | |
|---|---|---|
| **Syntax Description** | *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. |
| | | A sequence number can be any integer between 1 and 4294967295. |
| | | By default, the first rule in an ACL has a sequence number of 10. |
| | | If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. |
| | | Use the **resequence** command to reassign sequence numbers to rules. |
| | *source* | Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |
| | *destination* | Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **flow-label** *flow-label-value* | (Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575. |
| **fragments** | (Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments. |

| | |
|---|---|
| *icmp-message* | (Optional) ICMPv6 message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under the "ICMPv6 Message Types" section in the "Usage Guidelines" section. |
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: <br><br> • Protocol <br><br> • Source and destination addresses <br><br> • Source and destination port numbers, if applicable |

**Command Default**    None

**Command Modes**    IPv6 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

• Address and variable-length subnet mask—You can use an IPv6 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv6-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

  switch(config-ipv6-acl)# **permit icmp 2001:0db8:85a3::/48 any**

• Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv6-address*

  This syntax is equivalent to *IPv6-address*/128.

  This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-ipv6-acl)# permit icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

**ICMPv6 Message Types**

The *icmp-message* argument can be the ICMPv6 message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **beyond-scope**—Destination beyond scope
- **destination-unreachable**—Destination address is unreachable
- **echo-reply**—Echo reply
- **echo-request**—Echo request (ping)
- **header**—Parameter header problems
- **hop-limit**—Hop limit exceeded in transit
- **mld-query**—Multicast Listener Discovery Query
- **mld-reduction**—Multicast Listener Discovery Reduction
- **mld-report**—Multicast Listener Discovery Report
- **nd-na**—Neighbor discovery neighbor advertisements
- **nd-ns**—Neighbor discovery neighbor solicitations
- **next-header**—Parameter next header problems
- **no-admin**—Administration prohibited destination
- **no-route**—No route to destination
- **packet-too-big**—Packet too big
- **parameter-option**—Parameter option problems
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—Neighbor redirect
- **renum-command**—Router renumbering command
- **renum-result**—Router renumbering result
- **renum-seq-number**—Router renumbering sequence number reset
- **router-advertisement**—Neighbor discovery router advertisements
- **router-renumbering**—All router renumbering
- **router-solicitation**—Neighbor discovery router solicitations
- **time-exceeded**—All time exceeded messages
- **unreachable**—All unreachable

**Cisco Nexus 5500 Series NX-OS Security Command Reference** ■

■ **permit icmp (IPv6)**

**Examples**    This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules permitting all ICMP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit icmp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit icmp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

**Related Commands**

| Command | Description |
|---|---|
| **deny (IPv6)** | Configures a deny rule in an IPv6 ACL. |
| **ipv6 access-list** | Configures an IPv6 ACL. |
| **remark** | Configures a remark in an ACL. |

# permit ipv6 (IPv6)

To create an access control list (ACL) rule that permits IPv6 traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

**General Syntax**

[*sequence-number*] **permit ipv6** *source destination* [**dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

**no permit ipv6** *source destination* [**dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

**no** *sequence-number*

| Syntax Description | | |
|---|---|---|
| | *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. |
| | | A sequence number can be any integer between 1 and 4294967295. |
| | | By default, the first rule in an ACL has a sequence number of 10. |
| | | If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. |
| | | Use the **resequence** command to reassign sequence numbers to rules. |
| | *source* | Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |
| | *destination* | Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **flow-label** *flow-label-value* | (Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575. |

| | |
|---|---|
| **fragments** | (Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments. |
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |

- Protocol

- Source and destination addresses

- Source and destination port numbers, if applicable

**Command Default**    None

**Command Modes**    IPv6 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and variable-length subnet mask—You can use an IPv6 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv6-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

  ```
  switch(config-acl)# permit ipv6 2001:0db8:85a3::/48 any
  ```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv6-address*

**Cisco Nexus 5500 Series NX-OS Security Command Reference** ■

This syntax is equivalent to *IPv6-address*/128.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# permit ipv6 host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

**Examples**    This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules permitting all IPv6 traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit ipv6 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit ipv6 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named ipv6-eng-to-marketing with a rule that permits all IPv6 traffic from an IPv6-address object group named eng_ipv6 to an IPv6-address object group named marketing_group:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

**Related Commands**

| Command | Description |
|---------|-------------|
| **deny (IPv6)** | Configures a deny rule in an IPv6 ACL. |
| **ipv6 access-list** | Configures an IPv6 ACL. |
| **remark** | Configures a remark in an ACL. |

# permit sctp (IPv6)

To create an access control list (ACL) rule that permits IPv6 sctp traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

**General Syntax**

[*sequence-number*] **permit sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

**no permit sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

**no** *sequence-number*

| Syntax Description | | |
|---|---|---|
| | *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. |
| | | A sequence number can be any integer between 1 and 4294967295. |
| | | By default, the first rule in an ACL has a sequence number of 10. |
| | | If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. |
| | | Use the **resequence** command to reassign sequence numbers to rules. |
| | *source* | Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |
| | *destination* | Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |

| | |
|---|---|
| *operator port* [*port*] | (Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. |
| | The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. |
| | A second *port* argument is required only when the *operator* argument is a range. |
| | The *operator* argument must be one of the following keywords: |
| | &bull; **eq**—Matches only if the port in the packet is equal to the *port* argument. |
| | &bull; **gt**—Matches only if the port in the packet is greater than the *port* argument. |
| | &bull; **lt**—Matches only if the port in the packet is less than the *port* argument. |
| | &bull; **neq**—Matches only if the port in the packet is not equal to the *port* argument. |
| | &bull; **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument. |
| **portgroup** *portgroup* | (Optional) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. |
| | Use the **object-group ip port** command to create and change IP port-group objects. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **flow-label** *flow-label-value* | (Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575. |

| | |
|---|---|
| **fragments** | (Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments. |
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |

- Protocol
- Source and destination addresses
- Source and destination port numbers, if applicable

**Command Default**    None

**Command Modes**    IPv6 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and variable-length subnet mask—You can use an IPv6 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv6-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

  switch(config-acl)# **permit sctp 2001:0db8:85a3::/48 any**

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv6-address*

This syntax is equivalent to *IPv6-address*/128.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# permit sctp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

**Examples**    This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules permitting all SCTP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit sctp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit sctp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named ipv6-eng-to-marketing with a rule that permits all IPv6 traffic from an IPv6-address object group named eng_ipv6 to an IPv6-address object group named marketing_group:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit sctp addrgroup eng_ipv6 addrgroup marketing_group
```

**Related Commands**

| Command | Description |
|---|---|
| **deny (IPv6)** | Configures a deny rule in an IPv6 ACL. |
| **ipv6 access-list** | Configures an IPv6 ACL. |
| **remark** | Configures a remark in an ACL. |

# permit tcp (IPv6)

To create an access control list (ACL) rule that permits IPv6 TCP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | *flags* | **flow-label** *flow-label-value* | **fragments** | **log** | **established**]

**no permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | *flags* | **flow-label** *flow-label-value* | **fragments** | **log** | **established**]

**no** *sequence-number*

**Syntax Description**

| | |
|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. |
| | A sequence number can be any integer between 1 and 4294967295. |
| | By default, the first rule in an ACL has a sequence number of 10. |
| | If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. |
| | Use the **resequence** command to reassign sequence numbers to rules. |
| *source* | Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |
| *destination* | Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. |

| *operator port* [*port*] | (Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. |
|---|---|
| | The *port* argument can be the name or the number of a TCP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the "TCP Port Names" section in the "Usage Guidelines" section. |
| | A second *port* argument is required only when the *operator* argument is a range. |
| | The *operator* argument must be one of the following keywords: |
| | • **eq**—Matches only if the port in the packet is equal to the *port* argument. |
| | • **gt**—Matches only if the port in the packet is greater than the *port* argument. |
| | • **lt**—Matches only if the port in the packet is less than the *port* argument. |
| | • **neq**—Matches only if the port in the packet is not equal to the *port* argument. |
| | • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument. |
| **portgroup** *portgroup* | (Optional) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. |
| | Use the **object-group ip port** command to create and change IP port-group objects. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **established** | (Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection. |
| *flags* | (Optional) Rule matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: |
| | • **ack** |
| | • **fin** |
| | • **psh** |
| | • **rst** |
| | • **syn** |
| | • **urg** |

| | |
|---|---|
| **flow-label** *flow-label-value* | (Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575. |
| **fragments** | (Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments. |
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |

- Protocol
- Source and destination addresses
- Source and destination port numbers, if applicable

**Command Default**     None

**Command Modes**     IPv6 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**     A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and variable-length subnet mask—You can use an IPv6 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

    *IPv6-address/prefix-len*

    This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

    ```
    switch(config-acl)# permit tcp 2001:0db8:85a3::/48 any
    ```

• Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

**host** *IPv6-address*

This syntax is equivalent to *IPv6-address*/128.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

switch(config-acl)# **permit tcp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any**

• Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

### TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

• **bgp**—Border Gateway Protocol (179)
• **chargen**—Character generator (19)
• **cmd**—Remote commands (rcmd, 514)
• **daytime**—Daytime (13)
• **discard**—Discard (9)
• **domain**—Domain Name Service (53)
• **drip**—Dynamic Routing Information Protocol (3949)
• **echo**—Echo (7)
• **exec**—Exec (rsh, 512)
• **finger**—Finger (79)
• **ftp**—File Transfer Protocol (21)
• **ftp-data**—FTP data connections (2)
• **gopher**—Gopher (7)
• **hostname**—NIC hostname server (11)
• **ident**—Ident Protocol (113)
• **irc**—Internet Relay Chat (194)
• **klogin**—Kerberos login (543)
• **kshell**—Kerberos shell (544)
• **login**—Login (rlogin, 513)
• **lpd**—Printer service (515)
• **nntp**—Network News Transport Protocol (119)
• **pim-auto-rp**—PIM Auto-RP (496)
• **pop2**—Post Office Protocol v2 (19)
• **pop3**—Post Office Protocol v3 (11)
• **smtp**—Simple Mail Transport Protocol (25)

- **sunrpc**—Sun Remote Procedure Call (111)

- **tacacs**—TAC Access Control System (49)

- **talk**—Talk (517)

- **telnet**—Telnet (23)

- **time**—Time (37)

- **uucp**—Unix-to-Unix Copy Program (54)

- **whois**—WHOIS/NICNAME (43)

- **www**—World Wide Web (HTTP, 8)

**Examples**

This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules permitting all TCP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named ipv6-eng-to-marketing with a rule that permits all IPv6 TCP traffic from an IPv6-address object group named eng_ipv6 to an IPv6-address object group named marketing_group:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit tcp addrgroup eng_ipv6 addrgroup marketing_group
```

**Related Commands**

| Command | Description |
| --- | --- |
| **deny (IPv6)** | Configures a deny rule in an IPv6 ACL. |
| **ipv6 access-list** | Configures an IPv6 ACL. |
| **remark** | Configures a remark in an ACL. |

**Cisco Nexus 5500 Series NX-OS Security Command Reference**

# permit udp (IPv6)

To create an access control list (ACL) rule that permits IPv6 UDP traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

**General Syntax**

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

**no permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **flow-label** *flow-label-value* | **fragments** | **log**]

**no** *sequence-number*

| Syntax Description | | |
|---|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. | |
| | A sequence number can be any integer between 1 and 4294967295. | |
| | By default, the first rule in an ACL has a sequence number of 10. | |
| | If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. | |
| | Use the **resequence** command to reassign sequence numbers to rules. | |
| *source* | Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. | |
| *destination* | Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see the "Source and Destination" section in the "Usage Guidelines" section. | |

| | |
|---|---|
| *operator port* [*port*] | (Optional) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. |
| | The *port* argument can be the name or the number of a UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see the "UDP Port Names" section in the "Usage Guidelines" section. |
| | A second *port* argument is required only when the *operator* argument is a range. |
| | The *operator* argument must be one of the following keywords: |
| | • **eq**—Matches only if the port in the packet is equal to the *port* argument. |
| | • **gt**—Matches only if the port in the packet is greater than the *port* argument. |
| | • **lt**—Matches only if the port in the packet is less than the *port* argument. |
| | • **neq**—Matches only if the port in the packet is not equal to the *port* argument. |
| | • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument. |
| **portgroup** *portgroup* | (Optional) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. |
| | Use the **object-group ip port** command to create and change IP port-group objects. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords: |
| | • 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010. |
| | • **af11**—Assured Forwarding (AF) class 1, low drop probability (001010) |
| | • **af12**—AF class 1, medium drop probability (001100) |
| | • **af13**—AF class 1, high drop probability (001110) |
| | • **af21**—AF class 2, low drop probability (010010) |
| | • **af22**—AF class 2, medium drop probability (010100) |
| | • **af23**—AF class 2, high drop probability (010110) |
| | • **af31**—AF class 3, low drop probability (011010) |
| | • **af32**—AF class 3, medium drop probability (011100) |
| | • **af33**—AF class 3, high drop probability (011110) |
| | • **af41**—AF class 4, low drop probability (100010) |
| | • **af42**—AF class 4, medium drop probability (100100) |
| | • **af43**—AF class 4, high drop probability (100110) |
| | • **cs1**—Class-selector (CS) 1, precedence 1 (001000) |
| | • **cs2**—CS2, precedence 2 (010000) |
| | • **cs3**—CS3, precedence 3 (011000) |
| | • **cs4**—CS4, precedence 4 (100000) |
| | • **cs5**—CS5, precedence 5 (101000) |
| | • **cs6**—CS6, precedence 6 (110000) |
| | • **cs7**—CS7, precedence 7 (111000) |
| | • **default**—Default DSCP value (000000) |
| | • **ef**—Expedited Forwarding (101110) |
| **flow-label** *flow-label-value* | (Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575. |

| | |
|---|---|
| **fragments** | (Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments. |
| **log** | (Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: |

- Protocol
- Source and destination addresses
- Source and destination port numbers, if applicable

**Command Default**    None

**Command Modes**    IPv6 ACL configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    A newly created IPv6 ACL contains no rules.

When the device applies an IPv6 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and variable-length subnet mask—You can use an IPv6 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv6-address/prefix-len*

  This example shows how to specify the *source* argument with the IPv6 address and VLSM for the 2001:0db8:85a3:: network:

  ```
  switch(config-acl)# permit udp 2001:0db8:85a3::/48 any
  ```

- Host address—You can use the **host** keyword and an IPv6 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv6-address*

This syntax is equivalent to *IPv6-address*/128.

This example shows how to specify the *source* argument with the **host** keyword and the 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 address:

```
switch(config-acl)# permit udp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv6 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

**UDP Port Names**

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

- **biff**—Biff (mail notification, comsat, 512)
- **bootpc**—Bootstrap Protocol (BOOTP) client (68)
- **bootps**—Bootstrap Protocol (BOOTP) server (67)
- **discard**—Discard (9)
- **dnsix**—DNSIX security protocol auditing (195)
- **domain**—Domain Name Service (DNS, 53)
- **echo**—Echo (7)
- **isakmp**—Internet Security Association and Key Management Protocol (5)
- **mobile-ip**—Mobile IP registration (434)
- **nameserver**—IEN116 name service (obsolete, 42)
- **netbios-dgm**—NetBIOS datagram service (138)
- **netbios-ns**—NetBIOS name service (137)
- **netbios-ss**—NetBIOS session service (139)
- **non500-isakmp**—Internet Security Association and Key Management Protocol (45)
- **ntp**—Network Time Protocol (123)
- **pim-auto-rp**—PIM Auto-RP (496)
- **rip**—Routing Information Protocol (router, in.routed, 52)
- **snmp**—Simple Network Management Protocol (161)
- **snmptrap**—SNMP Traps (162)
- **sunrpc**—Sun Remote Procedure Call (111)
- **syslog**—System Logger (514)
- **tacacs**—TAC Access Control System (49)
- **talk**—Talk (517)
- **tftp**—Trivial File Transfer Protocol (69)
- **time**—Time (37)
- **who**—Who service (rwho, 513)
- **xdmcp**—X Display Manager Control Protocol (177)

**Examples**

This example shows how to configure an IPv6 ACL named acl-lab13-ipv6 with rules permitting all UDP traffic from the 2001:0db8:85a3:: and 2001:0db8:69f2:: networks to the 2001:0db8:be03:2112:: network:

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

This example shows how to configure an IPv6 ACL named ipv6-eng-to-marketing with a rule that permits all UDP traffic from an IPv6-address object group named eng_ipv6 to an IPv6-address object group named marketing_group:

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit udp addrgroup eng_ipv6 addrgroup marketing_group
```

**Related Commands**

| Command | Description |
| --- | --- |
| **deny (IPv6)** | Configures a deny rule in an IPv6 ACL. |
| **ipv6 access-list** | Configures an IPv6 ACL. |
| **remark** | Configures a remark in an ACL. |

# permit (MAC)

To create a MAC access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

**no permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

**no** *sequence-number*

**Syntax Description**

| | |
|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. |
| | A sequence number can be any integer between 1 and 4294967295. |
| | By default, the first rule in an ACL has a sequence number of 10. |
| | If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. |
| | Use the **resequence** command to reassign sequence numbers to rules. |
| *source* | Source MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section. |
| *destination* | Destination MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see "Source and Destination" in the "Usage Guidelines" section. |
| *protocol* | ( Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see "MAC Protocols" in the "Usage Guidelines" section. |
| **cos** *cos-value* | (Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the Class of Service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7. |
| **vlan** *vlan-id* | (Optional) Specifies that the rule matches only packets whose IEEE 802.1Q header contains the VLAN ID given. The *vlan-id* argument can be an integer from 1 to 4094. |

**Command Default**

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the switch assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

**Command Modes**

MAC ACL configuration mode

| Command History | Release | Modification |
|---|---|---|
| | 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    When the switch applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The switch enforces the first rule whose conditions are satisfied by the packet. When the conditions of more than one rule are satisfied, the switch enforces the rule with the lowest sequence number.

**Source and Destination**

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

  *MAC-address MAC-mask*

  This example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

  `switch(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any`

  This example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

  `switch(config-acl)# permit any 0060.3e00.0000 0000.0000.0000`

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each of the examples shows how to specify a source or destination by using the **any** keyword.

**MAC Protocols**

The *protocol* argument can be the MAC protocol number or a keyword. The protocol number is a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp**—Appletalk ARP (0x80f3)
- **appletalk**—Appletalk (0x809b)
- **decnet-iv**—DECnet Phase IV (0x6003)
- **diagnostic**—DEC Diagnostic Protocol (0x6005)
- **etype-6000**—Ethertype 0x6000 (0x6000)
- **etype-8042**—Ethertype 0x8042 (0x8042)
- **ip**—Internet Protocol v4 (0x0800)
- **lat**—DEC LAT (0x6004)
- **lavc-sca**—DEC LAVC, SCA (0x6007)
- **mop-console**—DEC MOP Remote console (0x6002)
- **mop-dump**—DEC MOP dump (0x6001)
- **vines-echo**—VINES Echo (0x0baf)

**Examples**     This example shows how to configure a MAC ACL named mac-ip-filter with a rule that permits all IPv4 traffic between two groups of MAC addresses:

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)#
```

**Related Commands**

| Command | Description |
|---|---|
| **deny (MAC)** | Configures a deny rule in a MAC ACL. |
| **mac access-list** | Configures a MAC ACL. |
| **remark** | Configures a remark in an ACL. |
| **show mac access-list** | Displays all MAC ACLs or one MAC ACL. |

# permit interface

To add interfaces for a user role interface policy, use the **permit interface** command. To remove interfaces, use the **no** form of this command.

> **permit interface** *interface-list*

> **no permit interface**

**Syntax Description**

| | |
|---|---|
| *interface-list* | List of interfaces that the user role has permission to access. |

**Command Default**    All interfaces

**Command Modes**    Interface policy configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    For permit interface statements to work, you need to configure a command rule to allow interface access, as shown in the following example:

```
switch(config-role)# rule number permit command configure terminal ; interface *
```

**Examples**    This example shows how to configure a range of interfaces for a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/2 - 8
```

This example shows how to configure a list of interfaces for a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5
```

This example shows how to remove an interface from a user role interface policy:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 1/2
```

**Related Commands**

| Command | Description |
|---|---|
| **interface policy deny** | Enters interface policy configuration mode for a user role. |

| Command | Description |
|---------|-------------|
| **role name** | Creates or specifies a user role and enters user role configuration mode. |
| **show role** | Displays user role information. |

# permit vlan

To add VLANs for a user role VLAN policy, use the **permit vlan** command. To remove VLANs, use the **no** form of this command.

> **permit vlan** *vlan-list*

> **no permit vlan**

**Syntax Description**

| | |
|---|---|
| *vlan-list* | List of VLANs that the user role has permission to access. |

**Command Default**    All VLANs

**Command Modes**    VLAN policy configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    For **permit vlan** statements to work, you need to configure a command **rule** to allow VLAN access, as shown in the following example:

```
switch(config-role)# rule number permit command configure terminal ; vlan *
```

**Examples**    This example shows how to configure a range of VLANs for a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

This example shows how to configure a list of VLANs for a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
```

This example shows how to remove a VLAN from a user role VLAN policy:

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
```

| Related Commands | Command | Description |
|---|---|---|
| | **vlan policy deny** | Enters VLAN policy configuration mode for a user role. |
| | **role name** | Creates or specifies a user role and enters user role configuration mode. |
| | **show role** | Displays user role information. |

# permit vrf

To add virtual routing and forwarding instances (VRFs) for a user role VRF policy, use the **permit vrf** command. To remove VRFs, use the **no** form of this command.

**permit vrf** *vrf-list*

**no permit vrf**

| Syntax Description | *vrf-list* | List of VRFs that the user role has permission to access. |
|---|---|---|

**Command Default**   All VRFs

**Command Modes**   VRF policy configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Examples**   This example shows how to configure a range of VRFs for a user role VRF policy:

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
```

**Related Commands**

| Command | Description |
|---|---|
| **vrf policy deny** | Enters VRF policy configuration mode for a user role. |
| **role name** | Creates or specifies a user role and enters user role configuration mode. |
| **show role** | Displays user role information. |

# permit vsan

To permit access to a VSAN policy for a user role, use the **permit vsan** command. To revert to the default VSAN policy configuration for a user role, use the **no** form of this command.

**permit vsan** *vsan-list*

**no permit vsan** *vsan-list*

| Syntax Description | *vsan-list* | Range of VSANs accessible to a user role. The range is from 1 to 4093. |
|---|---|---|
| | | You can separate the range using the following separators: |
| | | • **,** is a multirange separator; for example, 1-5, 10, 12, 100-201. |
| | | • **-** is a range separator; for example, 101-201. |

**Command Default**    None

**Command Modes**    User role configuration mode

**Command History**

| Release | Modification |
|---|---|
| 5.2(1)N1(1) | This command was introduced. |

**Usage Guidelines**    This command is enabled only after you deny a VSAN policy by using the **vsan policy deny** command.

**Examples**    This example shows how to permit access to a VSAN policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# permit vsan 10, 12, 100-104
switch(config-role-vsan)#
```

**Related Commands**

| Command | Description |
|---|---|
| **vsan policy deny** | Denies access to a VSAN policy for a user. |
| **role name** | Creates or specifies a user role and enters user role configuration mode. |
| **show role** | Displays user role information. |

■ **permit vsan**