I Commands

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

interface policy deny

To enter interface policy configuration mode for a user role, use the **interface policy deny** command. To revert to the default interface policy for a user role, use the **no** form of this command.

interface policy deny

no interface policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All interfaces

Command Modes

User role configuration mode

Command History

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

Examples

This example shows how to enter interface policy configuration mode for a user role:

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

This example shows how to revert to the default interface policy for a user role:

```
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
```

Related Commands

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

ip access-class

To create or configure an IPv4 access class to restrict incoming or outgoing traffic on a virtual terminal line (VTY), use the **ip access-class** command. To remove the access class, use the **no** form of this command.

ip access-class *access-list-name* {**in** | **out**}

no ip access-class *access-list-name* {**in** | **out**}

Syntax Description

access-list-name	Name of the IPv4 ACL class. The name can be a maximum of 64 characters. The name can contain characters, numbers, hyphens, and underscores. The name cannot contain a space or quotation mark.
in	Specifies that incoming connections be restricted between a particular Cisco Nexus 5000 Series switch and the addresses in the access list.
out	Specifies that outgoing connections be restricted between a particular Cisco Nexus 5000 Series switch and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode

Command History

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

Examples

This example shows how to configure an IP access class on a VTY line to restrict inbound packets:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# ip access-class VTY_ACCESS in
switch(config-line)#
```

This example shows how to remove an IP access class that restricts inbound packets:

```
switch(config)# line vty
switch(config-line)# no ip access-class VTY_ACCESS in
switch(config-line)#
```

Related Commands

Command	Description
access-class	Configures an access class for VTY.
copy running-config startup-config	Copies the running configuration to the startup configuration file.
show line	Displays the access lists for a particular terminal line.

Command	Description
show running-config aclmgr	Displays the running configuration of ACLs.
show startup-config aclmgr	Displays the startup configuration for ACLs.
ssh	Starts an SSH session using IPv4.
telnet	Starts a Telnet session using IPv4.

ip access-group

To apply an IPv4 access control list (ACL) to a Layer 3 interface as a router ACL, use the **ip access-group** command. To remove an IPv4 ACL from an interface, use the **no** form of this command.

ip access-group *access-list-name* **in**

no ip access-group *access-list-name* **in**

Syntax Description

access-list-name	Name of the IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
in	Specifies that the ACL applies to inbound traffic.

Command Default

None

Command Modes

Interface configuration mode
Subinterface configuration mode

Command History

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

Usage Guidelines

By default, no IPv4 ACLs are applied to a Layer 3 routed interface.

You can use the **ip access-group** command to apply an IPv4 ACL as a router ACL to the following interface types:

- VLAN interfaces
- Layer 3 Ethernet interfaces
- Layer 3 Ethernet subinterfaces
- Layer 3 Ethernet port-channel interfaces and subinterfaces
- Loopback interfaces
- Management interfaces

You can also use the **ip access-group** command to apply an IPv4 ACL as a router ACL to the following interface types:

- Layer 2 Ethernet interfaces
- Layer 2 Ethernet port-channel interfaces

However, an ACL applied to a Layer 2 interface with the **ip access-group** command is inactive unless the port mode changes to routed (Layer 3) mode.

If you delete the specified ACL from the device without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

A router ACL can be applied only to ingress traffic.

This command does not require a license.

Examples

This example shows how to apply an IPv4 ACL named ip-acl-01 to the Layer 3 Ethernet interface 2/1:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip access-group ip-acl-01 in
```

This example shows how to remove an IPv4 ACL named ip-acl-01 from Ethernet interface 2/1:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip access-group ip-acl-01 in
switch(config-if)# no ip access-group ip-acl-01 in
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs.
show ip access-lists	Shows either a specific IPv4 ACL or all IPv4 ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

ip access-list

To create an IPv4 access control list (ACL) or to enter IP access list configuration mode for a specific ACL, use the **ip access-list** command. To remove an IPv4 ACL, use the **no** form of this command.

ip access-list *access-list-name*

no ip access-list *access-list-name*

Syntax Description

access-list-name	Name of the IPv4 ACL, which can be up to 64 alphanumeric characters long. The name cannot contain a space or quotation mark.

Command Default

No IPv4 ACLs are defined by default.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Use IPv4 ACLs to filter IPv4 traffic.

When you use the **ip access-list** command, the switch enters IP access list configuration mode, where you can use the IPv4 **deny** and **permit** commands to configure rules for the ACL. If the specified ACL does not exist, the switch creates it when you enter this command.

Use the **ip access-group** command to apply the ACL to an interface.

Every IPv4 ACL has the following implicit rule as its last rule:

```
deny ip any any
```

This implicit rule ensures that the switch denies unmatched IP traffic.

IPv4 ACLs do not include additional implicit rules to enable the neighbor discovery process. The Address Resolution Protocol (ARP), which is the IPv4 equivalent of the IPv6 neighbor discovery process, uses a separate data link layer protocol. By default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Examples

This example shows how to enter IP access list configuration mode for an IPv4 ACL named ip-acl-01:

```
switch(config)# ip access-list ip-acl-01
switch(config-acl)#
```

Related Commands

Command	Description
access-class	Applies an IPv4 ACL to a VTY line.
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-group	Applies an IPv4 ACL to an interface.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.

ip arp event-history errors

To log Address Resolution Protocol (ARP) debug events into the event history buffer, use the **ip arp event-history errors** command.

ip arp event-history errors size {**disabled** | **large** | **medium** | **small**}

no ip arp event-history errors size {**disabled** | **large** | **medium** | **small**}

Syntax Description

size	Specifies the event history buffer size to configure.
disabled	Specifies that the event history buffer size is disabled.
large	Specifies that the event history buffer size is large.
medium	Specifies that the event history buffer size is medium.
small	Specifies that the event history buffer size is small. This is the default buffer size.

Command Default

By default, the event history buffer is small.

Command Modes

Global configuration mode

Command History

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

Examples

This example shows how to configure a medium ARP event history buffer:

```
switch(config)# ip arp event-history errors size medium
switch(config)#
```

This example shows how to set the ARP event history buffer to the default:

```
switch(config)# no ip arp event-history errors size medium
switch(config)#
```

Related Commands

Command	Description
show running-config arp all	Displays the ARP configuration, including the default configurations.

ip arp inspection log-buffer

To configure the Dynamic ARP Inspection (DAI) logging buffer size, use the **ip arp inspection log-buffer** command. To reset the DAI logging buffer to its default size, use the **no** form of this command.

ip arp inspection log-buffer entries *number*

no ip arp inspection log-buffer entries *number*

Syntax Description

entries *number*	Specifies the buffer size in a range of 1 to 1024 messages.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Before you use this command, make sure that you enable Dynamic Host Configuration Protocol (DHCP) snooping on the switch by using the **feature dhcp** command.

By default, the DAI logging buffer size is 32 messages.

Examples

This example shows how to configure the DAI logging buffer size:

```
switch# configure terminal
switch(config)# ip arp inspection log-buffer entries 64
switch(config)#
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.
feature dhcp	Enables DHCP snooping.
show ip arp inspection log	Displays the DAI log configuration.
show running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

ip arp inspection validate

To enable additional Dynamic ARP Inspection (DAI) validation, use the **ip arp inspection validate** command. To disable additional DAI, use the **no** form of this command.

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

ip arp inspection validate {**ip** [**dst-mac**] [**src-mac**]}

ip arp inspection validate {**src-mac** [**dst-mac**] [**ip**]}

no ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

no ip arp inspection validate {**ip** [**dst-mac**] [**src-mac**]}

no ip arp inspection validate {**src-mac** [**dst-mac**] [**ip**]}

Syntax Description

dst-mac	(Optional) Enables validation of the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. The device classifies packets with different MAC addresses as invalid and drops them.
ip	(Optional) Enables validation of the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. The device checks the sender IP addresses in all ARP requests and responses and checks the target IP addresses only in ARP responses.
src-mac	(Optional) Enables validation of the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. The devices classifies packets with different MAC addresses as invalid and drops them.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Before you use this command, make sure that you enable Dynamic Host Configuration Protocol (DHCP) snooping on the switch by using the **feature dhcp** command.

You must specify at least one keyword. If you specify more than one keyword, the order is irrelevant.

When you enable source MAC validation, an ARP packet is considered valid only if the sender Ethernet address in the packet body is the same as the source Ethernet address in the ARP frame header. When you enable destination MAC validation, an ARP request frame is considered valid only if the target Ethernet address is the same as the destination Ethernet address in the ARP frame header.

Examples

This example shows how to enable additional DAI validation:

```
switch# configure terminal
switch(config)# ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

This example shows how to disable additional DAI validation:

```
switch(config)# no ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping.
show ip arp inspection	Displays the DAI configuration status.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

ip arp inspection vlan

To enable Dynamic ARP Inspection (DAI) for a list of VLANs, use the **ip arp inspection vlan** command. To disable DAI for a list of VLANs, use the **no** form of this command.

ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit** | **all** | **none**}]

no ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit** | **all** | **none**}]

Syntax Description

vlan-list	VLANs on which DAI is active. The vlan-list argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.
logging	(Optional) Enables DAI logging for the VLANs specified. • **all**—Logs all packets that match Dynamic Host Configuration Protocol (DHCP) bindings • **none**—Does not log DHCP bindings packets (use this option to disable logging) • **permit**—Logs DHCP binding permitted packets
dhcp-bindings	Enables logging based on DHCP binding matches.
permit	Enables logging of packets permitted by a DHCP binding match.
all	Enables logging of all packets.
none	Disables logging.

Command Default

Logging of dropped packets

Command Modes

Global configuration

Command History

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

Usage Guidelines

By default, the device logs dropped packets inspected by DAI.

This command does not require a license.

Examples

This example shows how to enable DAI on VLANs 13, 15, and 17 through 23:

```
switch# configure terminal
switch(config)# ip arp inspection vlan 13,15,17-23
switch(config)#
```

Related Commands

Command	Description
ip arp inspection validate	Enables additional DAI validation.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

ip arp inspection trust

To configure a Layer 2 interface as a trusted ARP interface, use the **ip arp inspection trust** command. To configure a Layer 2 interface as an untrusted ARP interface, use the **no** form of this command.

ip arp inspection trust

no ip arp inspection trust

Syntax Description

This command has no arguments or keywords.

Command Default

By default, all interfaces are untrusted ARP interfaces.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

You can configure only Layer 2 Ethernet interfaces as trusted ARP interfaces.

This command does not require a license.

Examples

This example shows how to configure a Layer 2 interface as a trusted ARP interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip arp inspection trust
switch(config-if)#
```

Related Commands

Command	Description
show ip arp inspection	Displays the Dynamic ARP Inspection (DAI) configuration status.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

ip dhcp packet strict-validation

To enable the strict validation of Dynamic Host Configuration Protocol (DHCP) packets by the DHCP snooping feature, use the **ip dhcp packet strict-validation** command. To disable the strict validation of DHCP packets, use the **no** form of this command.

ip dhcp packet strict-validation

no ip dhcp packet strict-validation

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

You must enable DHCP snooping before you can use the **ip dhcp packet strict-validation** command.

Strict validation of DHCP packets checks that the DHCP options field in DCHP packets is valid, including the "magic cookie" value in the first four bytes of the options field. When strict validation of DHCP packets is enabled, the device drops DHCP packets that fail validation.

Examples

This example shows how to enable the strict validation of DHCP packets:

```
switch# configure terminal
switch(config)# ip dhcp packet strict-validation
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays the current DHCP configuration.

ip dhcp snooping

To globally enable Dynamic Host Configuration Protocol (DHCP) snooping on the device, use the **ip dhcp snooping** command. To globally disable DHCP snooping, use the **no** form of this command.

ip dhcp snooping

no ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

By default, DHCP snooping is globally disabled.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

The device preserves DHCP snooping configuration when you disable DHCP snooping with the **no ip dhcp snooping** command.

Examples

This example shows how to globally enable DHCP snooping:

```
switch# configure terminal
switch(config)# ip dhcp snooping
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping information option	Enables the insertion and removal of option-82 information for DHCP packets forwarded without the use of the DHCP relay agent.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

ip dhcp snooping information option

To enable the insertion and removal of option-82 information for Dynamic Host Configuration Protocol (DHCP) packets, use the **ip dhcp snooping information option** command. To disable the insertion and removal of option-82 information, use the **no** form of this command.

ip dhcp snooping information option

no ip dhcp snooping information option

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the device does not insert and remove option-82 information.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

Examples

This example shows how to globally enable DHCP snooping:

```
switch# configure terminal
switch(config)# ip dhcp snooping information option
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Globally enables DHCP snooping on the device.
ip dhcp snooping trust	Configures an interface as a trusted source of DHCP messages.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

ip dhcp snooping trust

To configure an interface as a trusted source of Dynamic Host Configuration Protocol (DHCP) messages, use the **ip dhcp snooping trust** command. To configure an interface as an untrusted source of DHCP messages, use the **no** form of this command.

ip dhcp snooping trust

no ip dhcp snooping trust

Syntax Description

This command has no arguments or keywords.

Command Default

By default, no interface is a trusted source of DHCP messages.

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).

You can configure DHCP trust on the following types of interfaces:

- Layer 3 Ethernet interfaces and subinterfaces
- Layer 2 Ethernet interfaces
- Private VLAN interfaces

Examples

This example shows how to configure an interface as a trusted source of DHCP messages:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip dhcp snooping trust
switch(config-if)#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping on the device.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

ip dhcp snooping verify mac-address

To enable Dynamic Host Configuration Protocol (DHCP) snooping for MAC address verification, use the **ip dhcp snooping verify mac-address** command. To disable DHCP snooping MAC address verification, use the **no** form of this command.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

By default, MAC address verification with DHCP snooping is not enabled.

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

If the device receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, address verification causes the device to drop the packet.

Examples

This example shows how to enable DHCP snooping for MAC address verification:

```
switch# configure terminal
switch(config)# ip dhcp snooping verify mac-address
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
show running-config dhcp	Displays the DHCP snooping configuration configuration.

ip dhcp snooping vlan

To enable Dynamic Host Configuration Protocol (DHCP) snooping on one or more VLANs, use the **ip dhcp snooping vlan** command. To disable DHCP snooping on one or more VLANs, use the **no** form of this command.

ip dhcp snooping vlan *vlan-list*

no ip dhcp snooping vlan *vlan-list*

Syntax Description

vlan-list	Range of VLANs on which to enable DHCP snooping. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges. Valid VLAN IDs are from 1 to 4094, except for the VLANs reserved for internal use. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, 20,70-100,142.

Command Default

By default, DHCP snooping is not enabled on any VLAN.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

To use this command, you must enable the DHCP snooping feature using the **feature dhcp** command.

Examples

This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252:

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

ip port access-group

To apply an IPv4 access control list (ACL) to an interface as a port ACL, use the **ip port access-group** command. To remove an IPv4 ACL from an interface, use the **no** form of this command.

ip port access-group *access-list-name* **in**

no ip port access-group *access-list-name* **in**

Syntax Description

access-list-name	Name of the IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters long.
in	Specifies that the ACL applies to inbound traffic.

Command Default

None

Command Modes

Interface configuration mode
Virtual Ethernet interface configuration mode

Command History

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

Usage Guidelines

By default, no IPv4 ACLs are applied to an interface.

You can use the **ip port access-group** command to apply an IPv4 ACL as a port ACL to the following interface types:

- Layer 2 Ethernet interfaces
- Layer 2 EtherChannel interfaces
- Virtual Ethernet interface

You can also apply an IPv4 ACL as a VLAN ACL. For more information, see the **match** command.

The switch applies port ACLs to inbound traffic only. The switch checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the switch without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply an IPv4 ACL named ip-acl-01 to Ethernet interface 1/2 as a port ACL:

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip port access-group ip-acl-01 in
```

This example shows how to remove an IPv4 ACL named ip-acl-01 from Ethernet interface 1/2:

```
switch(config)# interface ethernet 1/2
switch(config-if)# no ip port access-group ip-acl-01 in
switch(config-if)#
```

This example shows how to apply an IPv4 ACL named ip-acl-03 to the virtual Ethernet interface 1 as a port ACL:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ip port access-group ip-acl-03 in
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures avirtual Ethernet interface.
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs.
show ip access-lists	Shows either a specific IPv4 ACL or all IPv4 ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

ip source binding

To create a static IP source entry for a Layer 2 Ethernet interface, use the **ip source binding** command. To disable the static IP source entry, use the **no** form of this command.

ip source binding *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot*/[*QSFP-module/*]*port* | **port-channel** *channel-no*}

no ip source binding *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot*/[*QSFP-module/*]*port* | **port-channel** *channel-no*}

Syntax Description

IP-address	IPv4 address to be used on the specified interface. Valid entries are in dotted-decimal format.
MAC-address	MAC address to be used on the specified interface. Valid entries are in dotted-hexadecimal format.
vlan *vlan-id*	Specifies the VLAN associated with the IP source entry.
interface ethernet *slot*/[*QSFP-module/*]*port*	Specifies the Layer 2 Ethernet interface associated with the static IP entry. The slot number can be from 1 to 255. The *QSFP-module* number is from 1 to 4. The port number can be from 1 to 128. **Note** The *QSFP-module* number applies only to the QSFP+ Generic Expansion Module (GEM).
port-channel *channel-no*	Specifies the EtherChannel interface. The number can be from 1 to 4096.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	Support for the QSFP+ GEM was added.
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

By default, there are no static IP source entries.

To use this command, you must enable the Dynamic Host Configuration Protocol (DHCP) snooping feature using the **feature dhcp** command.

Examples

This example shows how to create a static IP source entry associated with VLAN 100 on Ethernet interface 2/3:

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
show ip verify source	Displays IP-to-MAC address bindings.
show interface	Displays interface configuration.
show running-config dhcp	Displays the DHCP snooping configuration information.

ip verify source dhcp-snooping-vlan

To enable IP Source Guard on a Layer 2 Ethernet interface, use the **ip verify source dhcp-snooping-vlan** command. To disable IP Source Guard on a Layer 2 Ethernet interface, use the **no** form of this command.

ip verify source dhcp-snooping-vlan

no ip verify source dhcp-snooping-vlan

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

Before you use this command, make sure that you enable Dynamic Host Configuration Protocol (DHCP) snooping on the switch by using the **feature dhcp** command.

IP Source Guard limits IP traffic on an interface to only those sources that have an IP-MAC address binding table entry or static IP source entry.

IP Source Guard is dependent upon DHCP snooping to build and maintain the IP-MAC address binding table or upon manual maintenance of static IP source entries.

This command does not require a license.

Examples

This example shows how to enable IP Source Guard on a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ip verify source dhcp-snooping-vlan
switch(config-if)#
```

This example shows how to disable IP Source Guard on a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ip verify source dhcp-snooping-vlan
switch(config-if)#
```

Related Commands

Command	Description
feature dhcp	Enables DHCP snooping on the switch.
ip source binding	Creates a static IP source entry for a Layer 2 Ethernet interface.
show ip verify source	Displays the IP-to-MAC address bindings for an interface.
show running-config dhcp	Displays the IP configuration in the running configuration.
show running-config interface ethernet	Displays the interface configuration in the running configuration.

ip verify unicast source reachable-via

To configure Unicast Reverse Path Forwarding (Unicast RPF) on an interface, use the **ip verify unicast source reachable-via** command. To remove Unicast RPF from an interface, use the **no** form of this command.

ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

no ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

Syntax Description

any	Specifies loose checking.
allow-default	(Optional) Specifies the MAC address to be used on the specified interface.
rx	Specifies strict checking.

Command Default

None

Command Modes

Interface configuration mode

Command History

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

Usage Guidelines

You can configure one of the following Unicast RPF modes on an ingress interface:

- Strict Unicast RPF mode—A strict mode check is successful when the following matches occur:
  - Unicast RPF finds a match in the Forwarding Information Base (FIB) for the packet source address.
  - The ingress interface through which the packet is received matches one of the Unicast RPF interfaces in the FIB match.

  If these checks fail, the packet is discarded. You can use this type of Unicast RPF check where packet flows are expected to be symmetrical.
- Loose Unicast RPF mode—A loose mode check is successful when a lookup of a packet source address in the FIB returns a match and the FIB result indicates that the source is reachable through at least one real interface. The ingress interface through which the packet is received is not required to match any of the interfaces in the FIB result.

This command does not require a license.

Examples

This example shows how to configure loose Unicast RPF checking on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ip verify unicast source reachable-via any
```

This example shows how to configure strict Unicast RPF checking on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ip verify unicast source reachable-via rx
```

Related Commands

Command	Description
show ip interface ethernet	Displays the IP-related information for an interface.
show running-config interface ethernet	Displays the interface configuration in the running configuration.
show running-config ip	Displays the IP configuration in the running configuration.

ipv6 access-class

To create or configure an IPv6 access class to restrict incoming or outgoing traffic on a virtual terminal line (VTY), use the **ipv6 access-class** command. To remove the access class, use the **no** form of this command.

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

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

Syntax Description

access-list-name	Name of the IPv6 ACL class. The name can be a maximum of 64 characters. The name can contain characters, numbers, hyphens, and underscores. The name cannot contain a space or quotation mark.
in	Specifies that incoming connections be restricted between a particular Cisco Nexus 5000 Series switch and the addresses in the access list.
out	Specifies that outgoing connections be restricted between a particular Cisco Nexus 5000 Series switch and the addresses in the access list.

Command Default

None

Command Modes

Line configuration mode

Command History

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

Examples

This example shows how to configure an IPv6 access class on a VTY line to restrict inbound packets:

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# ipv6 access-class VTY_I6ACCESS in
switch(config-line)#
```

This example shows how to remove an IPv6 access class that restricts inbound packets:

```
switch(config)# line vty
switch(config-line)# no ipv6 access-class VTY_I6ACCESS in
switch(config-line)#
```

Related Commands

Command	Description
access-class	Configures an access class for VTY.
copy running-config startup-config	Copies the running configuration to the startup configuration file.
show ipv6 access-class	Displays IPv6 access classes.

Command	Description
show line	Displays the access lists for a particular terminal line.
show running-config aclmgr	Displays the running configuration of ACLs.
show startup-config aclmgr	Displays the startup configuration for ACLs.
ssh6	Starts an SSH session using IPv6.
telnet6	Starts a Telnet session using IPv6.

ipv6 access-list

To create an IPv6 access control list (ACL) or to enter IP access list configuration mode for a specific ACL, use the **ipv6 access-list** command. To remove an IPv6 ACL, use the **no** form of this command.

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

Syntax Description

access-list-name	Name of the IPv6 ACL, which can be up to 64 alphanumeric characters long. The name cannot contain a space or quotation mark.

Command Default

No IPv6 ACLs are defined by default.

Command Modes

Global configuration mode

Command History

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

Usage Guidelines

Use IPv6 ACLs to filter IPv6 traffic.

When you use the **ipv6 access-list** command, the switch enters IP access list configuration mode, where you can use the IPv6 **deny** and **permit** commands to configure rules for the ACL. If the specified ACL does not exist, the switch creates it when you enter this command.

Every IPv6 ACL has the following implicit rule as its last rule:

```
deny ipv6 any any
```

This implicit rule ensures that the switch denies unmatched IP traffic.

Examples

This example shows how to enter IP access list configuration mode for an IPv6 ACL named ipv6-acl-01:

```
switch(config)# ipv6 access-list ipv6-acl-01
switch(config-ipv6-acl)#
```

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.

ipv6 port traffic-filter

To apply an IPv6 access control list (ACL) to an interface as a port ACL, use the **ipv6 port traffic-filter** command. To remove an IPv6 ACL from an interface, use the **no** form of this command.

ipv6 port traffic-filter *access-list-name* **in**

no ipv6 port traffic-filter *access-list-name* **in**

Syntax Description

access-list-name	Name of the IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
in	Specifies that the device applies the ACL to inbound traffic.

Command Default

None

Command Modes

Interface configuration mode
Virtual Ethernet interface configuration mode

Command History

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

Usage Guidelines

By default, no IPv6 ACLs are applied to an interface.

You can use the **ipv6 port traffic-filter** command to apply an IPv6 ACL as a port ACL to the following interface types:

- Ethernet interfaces
- EtherChannel interfaces
- Virtual Ethernet interface

You can also use the **ipv6 port traffic-filter** command to apply an IPv6 ACL as a port ACL to the following interface types:

- VLAN interfaces

Note You must enable VLAN interfaces globally before you can configure a VLAN interface. For more information, see the **feature interface-vlan** command.

The switch applies port ACLs to inbound traffic only. The switch checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the device without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply an IPv6 ACL named ipv6-acl to Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 port traffic-filter ipv6-acl in
switch(config-if)#
```

This example shows how to remove an IPv6 ACL named ipv6-acl from Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 port traffic-filter ipv6-acl in
switch(config-if)#
```

This example shows how to apply an IPv6 ACL named ipv6-acl-03 to a specific virtual Ethernet interface:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ipv6 port traffic-filter ipv6-acl-03 in
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
ipv6 access-list	Configures an IPv6 ACL.
show access-lists	Displays all ACLs.
show ipv6 access-lists	Shows either a specific IPv6 ACL or all IPv6 ACLs.

ipv6 traffic-filter

To apply an IPv6 access control list (ACL) to an interface, use the **ipv6 traffic-filter** command. To remove an IPv6 ACL from an interface, use the **no** form of this command.

ipv6 traffic-filter *access-list-name* **in**

no ipv6 traffic-filter *access-list-name* **in**

Syntax Description

access-list-name	Name of the IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
in	Specifies that the device applies the ACL to inbound traffic.

Command Default

None

Command Modes

Interface configuration mode
Virtual Ethernet interface configuration mode

Command History

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

Usage Guidelines

By default, no IPv6 ACLs are applied to an interface.

You can use the **ipv6 traffic-filter** command to apply an IPv6 ACL to the following interface types:

- Ethernet interfaces
- EtherChannel interfaces
- Virtual Ethernet interface
- VLAN interfaces

Note You must enable VLAN interfaces globally before you can configure a VLAN interface. For more information, see the **feature interface-vlan** command.

The switch applies ACLs to inbound traffic only. The switch checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the switch continues to process the packet. If the first matching rule denies the packet, the switch drops the packet and returns an ICMP host-unreachable message.

If you delete the specified ACL from the device without removing the ACL from an interface, the deleted ACL does not affect traffic on the interface.

Examples

This example shows how to apply an IPv6 ACL named ipv6-acl to Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 traffic-filter ipv6-acl in
switch(config-if)#
```

This example shows how to remove an IPv6 ACL named ipv6-acl from Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 traffic-filter ipv6-acl in
switch(config-if)#
```

This example shows how to apply an IPv6 ACL named ipv6-acl-03 to a specific virtual Ethernet interface:

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ipv6 traffic-filter ipv6-acl-03 in
switch(config-if)#
```

Related Commands

Command	Description
interface vethernet	Configures a virtual Ethernet interface.
ipv6 access-list	Configures an IPv6 ACL.
show access-lists	Displays all ACLs.
show ipv6 access-lists	Shows either a specific IPv6 ACL or all IPv6 ACLs.