I Commands

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

identity policy

To create or specify an identity policy and enter identity policy configuration mode, use the **identity policy** command. To remove an identity policy, use the **no** form of this command.

identity policy *policy-name*

no identity policy *policy-name*

Syntax Description

policy-name	Name for the identity policy. The name is case sensitive, alphanumeric, and has a maximum of 100 characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to create an identity policy and enter identity policy configuration mode:

```
switch# configure terminal
switch(config)# identity policy AdminPolicy
switch(config-id-policy)#
```

This example shows how to remove an identity policy:

```
switch# configure terminal
switch(config)# no identity policy AdminPolicy
```

Related Commands

Command	Description
show identity policy	Displays identity policy information.

identity profile eapoudp

To create the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) identity profile and enter identity profile configuration mode, use the **identity profile eapoupd** command. To remove the EAPoUPD identity profile configuration, use the **no** form of this command.

identity profile eapoudp

no identity profile eapoudp

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to create the EAPoUDP identity profile and enter identity profile configuration mode:

```
switch# configure terminal
switch(config)# identity profile eapoudp
switch(config-id-policy)#
```

This example shows how to remove the EAPoUDP identity profile configuration:

```
switch# configure terminal
switch(config)# no identity profile eapoudp
```

Related Commands

Command	Description
show identity profile	Displays identity profile information.

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.

Defaults

All interfaces

Command Modes

User role configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command denies all interfaces to the user role except for those that you allow using the **permit interface** command in user role interface policy configuration mode.

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
permit interface	Permits interfaces in a role interface policy.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

ip access-class

To configure a virtual teletype (VTY) access control list (ACL) to control access to all IPv4 traffic over all VTY lines in the ingress or egress direction, use the **ip access-class** command. To remove the VTY ACL, use the **no** form of this command.

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

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

Syntax Description

name	Access class name. The name can be up to 64 alphanumeric, case-sensitive characters. Names cannot contain a space or quotation mark.
in	Specifies the incoming packets.
out	Specifies the outgoing packets.

Defaults

None

Command Modes

Global configuration (config)

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

The VTY ACL feature restricts all traffic for all VTY lines. You cannot specify different traffic restrictions for different VTY lines.

Any router ACL can be configured as a VTY ACL.

This command does not require a license.

Examples

This example shows how to configure a VTY ACL to control access to all IPv4 traffic over all VTY lines :

```
switch# configure terminal
switch(config)# ip access-list vtyacl
switch(config-ip-acl)# exit
switch(config)# line vty
switch(config-line)# ip access-class vtyacl out
switch(config-line)#
```

This example shows how to remove the VTY ACL from all IPv4 traffic over all VTY lines :

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# no ip access-class vtyacl out
switch(config-line)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
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-group

To apply an IPv4 access control list (ACL) to an 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** | **out**}

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

Syntax Description

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

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

By default, no IPv4 ACLs are applied to an 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

Note You must enable VLAN interfaces globally before you can configure a VLAN interface. For more information, see the **feature interface-vlan** command in the *Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*.

- Layer 3 Ethernet interfaces
- Layer 3 Ethernet subinterfaces
- Layer 3 Ethernet port-channel interfaces and subinterfaces
- Tunnels
- 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. To apply an IPv4 ACL as a port ACL, use the **ip port access-group** command.

The device applies router ACLs on either outbound or inbound traffic. When the device applies an ACL to inbound traffic, the device checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the device continues to process the packet. If the first matching rule denies the packet, the device drops the packet and returns an ICMP host-unreachable message.

For outbound access lists, after receiving and routing a packet to an interface, the device checks the ACL. If the first matching rule permits the packet, the device sends the packet to its destination. If the first matching rule denies the packet, the device 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.

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
ip port access-group	Applies an IPv4 ACL as a port 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. The name has a maximum of 64 alphanumeric, case-sensitive characters but cannot contain a space or quotation mark.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

No IPv4 ACLs are defined by default.

Use IPv4 ACLs to filter IPv4 traffic.

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

Use the **ip access-group** command to apply the ACL to an interface as a router ACL. Use the **ip port access-group** command to apply the ACL to an interface as a port ACL.

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

```
deny ip any any
```

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

Unlike IPv6 ACLs, 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.

Use the **statistics per-entry** command to configure the device to record statistics for each rule in an IPv4 ACL. The device does not record statistics for implicit rules. To record statistics for packets that would match the implicit **deny ip any any** rule, you must explicitly configure an identical rule.

This command does not require a license.

Examples

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

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

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
ip access-group	Applies an IPv4 ACL to an interface as a router ACL.
ip port access-group	Applies an IPv4 ACL to an interface as a port ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.

ip arp inspection filter

To apply an ARP access control list (ACL) to a list of VLANs, use the **ip arp inspection filter** command. To remove the ARP ACL from the list of VLANs, use the **no** form of this command.

ip arp inspection filter *acl-name* **vlan** *vlan-list*

no ip arp inspection filter *acl-name* **vlan** *vlan-list*

Syntax Description

acl-name	Name of the ARP ACL, which can be up to 64 alphanumeric, case-sensitive characters.
vlan *vlan-list*	Specifies the VLANs to be filtered by the ARP ACL. 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.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to apply an ARP ACL named arp-acl-01 to VLANs 15 and 37 through 48:

```
switch# configure terminal
switch(config)# ip arp inspection filter arp-acl-01 vlan 15,37-48
switch(config)#
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip arp inspection vlan	Enables Dynamic ARP Inspection (DAI) for a specified list of VLANs.
show ip arp inspection	Displays the DAI configuration status.
show running-config dhcp	Displays DHCP snooping configuration, including the DAI configuration.

ip arp inspection log-buffer

To configure the Dynamic ARP Inspection (DAI) logging buffer size or the number of logs per interval, 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* **| logs** *number***}**

no ip arp inspection log-buffer {entries *number* **| logs** *number***}**

Syntax Description

entries *number*	Specifies the buffer size in a range of 0 to 1024 messages.
logs *number*	Specifies the number of logs per interval in a range of 0 to 1024 entries.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

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)#
```

This example shows how to configure the number of logs for Dynamic ARP Inspection:

```
switch# configure terminal
switch(config)# ip arp inspection log-buffer logs 6
switch(config)#
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.
show ip arp inspection	Displays the DAI configuration status.
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.

Defaults

By default, all interfaces are untrusted ARP interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
4.0(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 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 {[**dst-mac**] **ip** [**src-mac**]}

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

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

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

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

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.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

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)#
```

Related Commands

Command	Description
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 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.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

By default, the device does not log 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 dhcp packet strict-validation

To enable the strict validation of 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.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

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 the DHCP snooping feature on the device.
ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
ip dhcp snooping	Globally enables DHCP snooping on the device.
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 relay

To enable the DHCP relay agent, use the **ip dhcp relay** command. To disable the DHCP relay agent, use the **no** form of this command.

ip dhcp relay

no ip dhcp relay

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.2(1)	This command was introduced to replace the **service dhcp** command.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to globally enable DHCP snooping:

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

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp relay address	Configures an IP address of a DHCP server on an interface.
ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays the DHCP snooping configuration, including the IP source guard configuration.

ip dhcp relay address

To configure the IP address of a DHCP server on an interface, use the **ip dhcp relay address** command. To remove the DHCP server IP address, use the **no** form of this command.

ip dhcp relay address *IP-address* [**use-vrf** *vrf-name*]

no ip dhcp relay address *IP-address* [**use-vrf** *vrf-name*]

Syntax Description

IP-address	IPv4 address of the DHCP server.
use-vrf *vrf-name*	Specifies the virtual routing and forwarding instance (VRF) that the DHCP server is within, where the *vrf-name* argument is the name of the VRF. The VRF membership of the interface connected to the DHCP server determines the VRF that the DHCP is within.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
5.0(2)	Added support for the **use-vrf** *vrf-name* option.
4.0(3)	Up to four **ip dhcp relay address** commands can be added to the configuration of a Layer 3 Ethernet interface or subinterface.
4.0(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 up to four DHCP server IP addresses on Layer 3 Ethernet interfaces and subinterfaces, VLAN interfaces, and Layer 3 port channels. In Cisco NX-OS Release 4.0.2 and earlier releases, you can configure only one DHCP server IP address on an interface.

When an inbound DHCP BOOTREQUEST packet arrives on the interface, the relay agent forwards the packet to all DHCP server IP addresses specified on that interface. The relay agent forwards replies from all DHCP servers to the host that sent the request.

This command does not require a license.

Examples

This example shows how to configure two IP addresses for DHCP servers so that the relay agent can forward BOOTREQUEST packets received on the specified Layer 3 Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)# ip dhcp relay address 10.132.7.175
switch(config-if)#
```

This example shows how to configure the IP address of a DHCP server on a VLAN interface:

```
switch# configure terminal
switch(config)# interface vlan 13
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)#
```

This example shows how to configure the IP address of a DHCP server on a Layer 3 port-channel interface:

```
switch# configure terminal
switch(config)# interface port-channel 7
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)#
```

Related Commands

Command	Description
ip dhcp relay	Enables or disables the DHCP relay agent.
ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
ip dhcp relay information option vpn	Enables VRF support for the DHCP relay agent.
ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays the DHCP snooping configuration, including the IP source guard configuration.

ip dhcp relay information option

To enable the device to insert and remove option-82 information on DHCP packets forwarded by the relay agent, use the **ip dhcp relay information option** command. To disable the insertion and removal of option-82 information, use the **no** form of this command.

ip dhcp relay information option

no ip dhcp relay information option

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the device does not insert and remove option-82 information on DHCP packets forwarded by the relay agent.

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to enable the DHCP relay agent to insert and remove option-82 information to and from packets it forwards:

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

Related Commands

Command	Description
ip dhcp relay	Enables or disables the DHCP relay agent.
ip dhcp relay address	Configures the IP address of a DHCP server on an interface.
ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.
ip dhcp snooping	Globally enables DHCP snooping 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.
show running-config dhcp	Displays the DHCP snooping configuration, including the IP source guard configuration.

ip dhcp relay information option vpn

To enable VRF support for the DHCP relay agent, use the **ip dhcp relay information option vpn** command. To disable VRF support, use the **no** form of this command.

ip dhcp relay information option vpn

no ip dhcp relay information option vpn

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the device does not support forwarding of DHCP requests to DHCP servers in different VRFs than the VRF that the DHCP client belongs to.

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable Option-82 information insertion for the DHCP relay agent (see the **ip dhcp relay information option** command).

You can configure the DHCP relay agent to forward DHCP broadcast messages from clients in one VRF to DHCP servers in a different VRF. By using a single DHCP server to provide DHCP support to clients in multiple VRFs, you can conserve IP addresses by using a single IP address pool rather than one for each VRF.

If a DHCP request arrives on an interface that you have configured with a DHCP relay address and VRF information and the address of the DCHP server belongs to a network on an interface that is a member of a different VRF, the device inserts Option-82 information in the request and forwards it to the DHCP server in the server VRF. The Option-82 information that the devices adds to a DHCP request relayed to a different VRF includes the following:

- VPN identifier—Contains the name of the VRF that the interface that receives the DHCP request is a member of.
- Link selection—Contains the subnet address of the interface that receives the DHCP request.
- Server identifier override—Contains the IP address of the interface that receives the DHCP request.

When the devices receives the DHCP response message, it strips off the Option-82 information and forwards the response to the DHCP client in the client VRF.

This command does not require a license.

Examples

This example shows how to enable VRF support for the DHCP relay agent, which is dependent upon enabling Option-82 support for the DHCP relay agent, and how to configure a DHCP server address on a Layer 3 interface when the DHCP server is in a VRF named SiteA:

```
switch# configure terminal
switch(config)# ip dhcp relay information option
switch(config)# ip dhcp relay information option vpn
switch(config)# interface ethernet 1/3
switch(config-if)# ip dhcp relay address 10.43.87.132 use-vrf SiteA
switch(config-if)#
```

Related Commands

Command	Description
ip dhcp relay	Enables or disables the DHCP relay agent.
ip dhcp relay address	Configures the IP address of a DHCP server on an interface.
ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show running-config dhcp	Displays the DHCP snooping configuration, including the IP source guard configuration.

ip dhcp relay subnet-broadcast

To configure the Cisco NX-OS device to support the relaying of Dynamic Host Configuration Protocol (DHCP) packets from clients to a subnet broadcast IP address, use the **ip dhcp relay subnet-broadcast** command. To revert to the default behavior, use the **no** form of this command.

ip dhcp relay subnet-broadcast

no ip dhcp relay subnet-broadcast

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration mode (config-if)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

DHCP smart relay and DHCP subnet broadcast support are limited to the first 100 IP addresses of the interface on which they are enabled.

You must configure a helper address on the interface in order to use DHCP smart relay and DHCP subnet broadcast support.

DHCP smart relay and DHCP subnet broadcast support are limited to the first 100 IP addresses of the interface on which they are enabled.

In a vPC environment with DHCP smart relay enabled, the subnet of the primary and secondary addresses of an interface should be the same on both Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to configure the Cisco NX-OS device to support the relaying of DHCP packets from clients to a subnet broadcast IP address:

```
switch# configure terminal
switch(config)# interface ethernet 3/2
switch(config-if)# ip dhcp relay subnet-broadcast
switch(config-if)

This example shows how to remove configuration for relaying of DHCP packets from clients
to a subnet broadcast IP address:

switch(config)# interface ethernet 3/2
switch(config-if)# no ip dhcp relay subnet-broadcast
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP feature on the device.
ip dhcp relay	Enable the DHCP relay agent.

ip dhcp relay sub-option type cisco

To enable DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions, use the **ip dhcp relay sub-option type cisco** command. To disable DHCP's use of these proprietary numbers, use the **no** form of this command.

ip dhcp relay sub-option type cisco

no ip dhcp relay sub-option type cisco

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled. DHCP uses RFC numbers 5, 11, and 151 for the link selection, server ID override, and VRF name/VPN ID suboptions, respectively.

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions:

```
switch# configure terminal
switch(config)# ip dhcp relay sub-option type cisco
switch(config)#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp relay	Enables the DHCP relay agent.
ip dhcp relay address	Configures an IP address of a DHCP server on an interface.
ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays the DHCP snooping configuration, including the IP source guard configuration.

ip dhcp smart-relay

To enable Dynamic Host Configuration Protocol (DHCP) smart relay on a Layer 3 interface, use the **ip dhcp smart-relay** command. To disable DHCP smart relay on a Layer 3 interface, use the **no** form of this command.

ip dhcp smart-relay

no ip dhcp smart-relay

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration mode (config-if)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

The DHCP smart relay agent can be configured independently in default and nondefault VDCs.

Before using the **ip dhcp smart-relay global command, you must** enable the IP DHCP relay agent using the **ip dhcp relay command.**

DHCP smart relay and DHCP subnet broadcast support are limited to the first 100 IP addresses of the interface on which they are enabled.

You must configure a helper address on the interface in order to use DHCP smart relay and DHCP subnet broadcast support.

DHCP smart relay and DHCP subnet broadcast support are limited to the first 100 IP addresses of the interface on which they are enabled.

A maximum of 10,000 clients can use DHCP smart relay at any given time.

In a vPC environment with DHCP smart relay enabled, the subnet of the primary and secondary addresses of an interface should be the same on both Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to enable DHCP smart relay on a Layer 3 interface:

```
switch# configure terminal
switch(config)# interface ethernet 7/2
switch(config-if)# ip dhcp smart-relay
switch(config-if)#
```

This example shows how to disable DHCP smart relay on a Layer 3 interface:

```
switch# configure terminal
switch(config)# interface ethernet 7/2
switch(config-if)# no ip dhcp smart-relay
switch(config-if)#
```

Related Commands

Command	Description
ip dhcp smart-relay global	Enables the DHCP smart relay globally on the Cisco NX-OS device.
ip dhcp relay	Enable the DHCP relay agent.

ip dhcp smart-relay global

To enable Dynamic Host Configuration Protocol (DHCP) smart relay globally on the Cisco NX-OS device, use the **ip dhcp smart-relay global** command. To disable DHCP smart relay globally on the Cisco NX-OS device, use the **no** form of this command.

ip dhcp smart-relay global

no ip dhcp smart-relay global

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

The DHCP smart relay agent can be configured independently in default and nondefault VDCs.

Before using the **ip dhcp smart-relay global command, you must** enable the IP DHCP relay agent using the **ip dhcp relay command.**

DHCP smart relay and DHCP subnet broadcast support are limited to the first 100 IP addresses of the interface on which they are enabled.

You must configure a helper address on the interface in order to use DHCP smart relay and DHCP subnet broadcast support.

A maximum of 10,000 clients can use DHCP smart relay at any given time.

In a vPC environment with DHCP smart relay enabled, the subnet of the primary and secondary addresses of an interface should be the same on both Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to enable DHCP smart relay globally on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# ip dhcp relay
switch(config)# ip dhcp smart-relay global
switch(config)#
```

This example shows how to disable DHCP smart relay globally on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# no ip dhcp smart-relay global
switch(config)#
```

Related Commands

Command	Description
ip dhcp smart-relay	Enables DHCP smart relay on a Layer 3 interface.
ip dhcp relay	Enable the DHCP relay agent.

ip dhcp snooping

To globally enable 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.

Defaults

By default, DHCP snooping is globally disabled.

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

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

This command does not require a license.

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 relay	Enables or disables the DHCP relay agent.
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 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.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

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
ip dhcp relay information option	Enables the insertion and removal of option-82 information from DHCP packets forwarded by the DHCP relay agent.
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 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.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
4.0(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

This command does not require a license.

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 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 verify mac-address	Enables MAC address verification as part of DHCP snooping.
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.

Command	Description
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 DHCP snooping 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.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(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 (see the **feature dhcp** command).

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

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
ip dhcp relay	Enables or disables the DHCP relay agent.
ip dhcp snooping	Globally enables DHCP snooping 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.

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.

ip dhcp snooping vlan

To enable DHCP snooping 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 (see the "Examples" section). Valid VLAN IDs are from 1 to 4096.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

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
ip dhcp snooping	Globally enables DHCP snooping 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 verify mac-address	Enables MAC address verification as part of DHCP snooping.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

ip forward-protocol udp

To enable the UDP relay feature, use the **ip forward-protocol udp** command.

ip forward-protocol udp [*port-range*]

no ip forward-protocol udp [*port-range*]

Syntax Description

port-range	Specifies the range of UDP ports to enable the UDP relay feature. The range is from 0 to 65535.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to enable the UDP relay feature:

```
switch# config t
switch(config)# ip forward-protocol udp
```

This example shows how to disable the UDP relay feature:

```
switch# config t
switch(config)# no ip forward-protocol udp
```

Related Commands

Command	Description
ip udp relay subnet-broadcast	Enables the UDP relay feature for the subnet broadcasts.
object-group udp relay ip address	Configures an object group containing IP addresses.

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.
in	Specifies that the ACL applies to inbound traffic.

Defaults

in

Command Modes

Interface configuration

Command History

Release	Modification
4.0(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 Ethernet port-channel interfaces

You can also use the **ip port access-group** command to apply an IPv4 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 in the *Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*.

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

However, an ACL applied to a Layer 3 interface with the **ip port access-group** command is inactive unless the port mode changes to access or trunk (Layer 2) mode. To apply an IPv4 ACL as a router ACL, use the **ip access-group** command.

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

The device applies port ACLs to inbound traffic only. The device checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the device continues to process the packet. If the first matching rule denies the packet, the device 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.

If MAC packet classification is enabled on a Layer 2 interface, you cannot use the **ip port access-group** command on the interface.

This command does not require a license.

Examples

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

```
switch# configure terminal
switch(config)# interface ethernet 2/1
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 2/1:

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

This example shows how to view the configuration of an Ethernet interface and the error message that appears if you try to apply an IPv4 port ACL to the interface when MAC packet classification is enabled:

```
switch(config)# show running-config interface ethernet 2/3

!Command: show running-config interface Ethernet2/3
!Time: Wed Jun 24 13:06:49 2009

version 4.2(1)

interface Ethernet2/3
  ip access-group ipacl in
  mac port access-group macacl
  switchport
  mac packet-classify

switch(config)# interface ethernet 2/3
switch(config-if)# ip port access-group ipacl in
ERROR: The given policy cannot be applied as mac packet classification is enable
d on this port
switch(config-if)#
```

Related Commands

Command	Description
ip access-group	Applies an IPv4 ACL to an interface as a router ACL.
ip access-list	Configures an IPv4 ACL.

Command	Description
mac packet-classify	Enables MAC packet classification on a Layer 2 interface.
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.
statistics per-entry	Enables collection of statistics for each entry in an ACL.

ip radius source-interface

To assign a global source interface for the RADIUS server groups, use the **ip radius source-interface** command. To revert to the default, use the **no** form of this command.

ip radius source-interface *interface*

no ip radius source-interface

Syntax Description

interface	Source interface. The supported interface types are **ethernet**, **loopback**, and **mgmt 0**.

Defaults

Any available interface

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the global source interface for RADIUS server groups:

```
switch# configure terminal
switch(config)# ip radius source-interface mgmt 0
```

This example shows how to remove the global source interface for RADIUS server groups:

```
switch# configure terminal
switch(config)# no ip radius source-interface
```

Related Commands

Command	Description
show radius-server groups	Displays the RADIUS server group configuration.

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/port*

no ip source binding *IP-address MAC-address* **vlan** *vlan-id* **interface ethernet** *slot/port*

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/port*	Specifies the Layer 2 Ethernet interface associated with the static IP entry.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

By default, there are no static IP source entries.

This command does not require a license.

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
ip verify source dhcp-snooping-vlan	Enables IP Source Guard on an interface.
show ip verify source	Displays IP-to-MAC address bindings.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

ip tacacs source-interface

To assign a global source interface for the TACACS+ server groups, use the **ip tacacs source-interface** command. To revert to the default, use the **no** form of this command.

ip tacacs source-interface *interface*

no ip tacacs source-interface

Syntax Description

interface	Source interface. The supported interface types are **ethernet**, **loopback**, and **mgmt 0**.

Defaults

Any available interface

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

This command does not require a license.

Examples

This example shows how to configure the global source interface for TACACS+ server groups:

```
switch# configure terminal
switch(config)# ip tacacs source-interface mgmt 0
```

This example shows how to remove the global source interface for TACACS+ server groups:

```
switch# configure terminal
switch(config)# no ip tacacs source-interface
```

Related Commands

Command	Description
feature tacacs+	Enables the TACACS+ feature.
show tacacs-server groups	Displays the TACACS+ server group configuration.

ip udp relay addrgroup

To associate an object group with an L3 interface, use the **ip udp relay addrgroup** command.

ip udp relay addrgroup *object-grp-name*

no ip udp relay addrgroup *object-grp-name*

Syntax Description

object-grp-name	Specifies the name of the object group.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must configure an object group by using the **object-group udp relay ip address** command.

Examples

This example shows how to associate an object group with an L3 interface:

```
switch(config)# interface ethernet e0/0
switch(config-if)# ip udp relay addrgroup udprelay1
```

This example shows how to disassociate the object group:

```
switch(config-if)# no ip udp relay addrgroup udprelay1
```

Related Commands

Command	Description
ip forward-protocol udp	Enables the UDP relay feature.
object-group udp relay ip address	Configures the object group.

ip udp relay subnet-broadcast

To enable the UDP relay feature on subnet broadcast, use the **ip udp relay subnet-broadcast** command.

ip udp relay subnet-broadcast

no ip udp relay subnet-broadcast

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the UDP relay feature by using the **ip forward-protocol udp** command and associate the object group with an L3 interface.

Examples

This example shows how to enable the UDP relay feature on the subnet broadcast:

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# ip forward-protocol udp
switch(config)# object-group udp relay ip address udprelay1
switch(config-udp-ogroup)# host 20.1.2.2
switch(config-udp-ogroup)# 30.1.1.1 255.255.255.0
switch(config-udp-ogroup)# 40.1.1.1/24
switch(config-udp-ogroup)# exit
switch(config)# interface ethernet e0/0
switch(config-if)# ip udp relay addrgroup udprelay1
switch(config-if)# ip udp relay subnet-broadcast
switch(config-if)# exit
```

This example shows how to disable the UDP relay feature on the subnet broadcast:

```
switch(config-if)# no ip udp relay subnet-broadcast
```

Related Commands

Command	Description
ip forward-protocol udp	Enables the UDP relay feature.
object-group udp relay ip address	Configures an object group containing IP addresses.

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 an 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.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

By default, IP Source Guard is not enabled on any interface.

This command does not require a license.

Examples

This example shows how to enable IP Source Guard on an interface:

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

Related Commands

Command	Description
ip source binding	Creates a static IP source entry for the specified Ethernet interface.
show ip verify source	Displays IP-to-MAC address bindings.

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.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can configure one 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.
show startup-config interface ethernet	Displays the interface configuration in the startup configuration.
show startup-config ip	Displays the IP configuration in the startup configuration.

ipv6 access-class

To configure a virtual type (VTY) access control list (ACL) to control access to all IPv6 traffic over all VTY lines in the ingress or egress direction, use the **ipv6 access-class** command. To remove the VTY ACL control access from the traffic over all VTY lines , use the **no** form of this command.

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

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

Syntax Description

name	Access class name. The name can be up to 64 alphanumeric, case-sensitive characters. Names cannot contain a space or quotation mark.
in	Specifies the incoming packets.
out	Specifies the outgoing packets.

Defaults

None

Command Modes

Global configuration (config)

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

The VTY ACL feature restricts all traffic for all VTY lines. You cannot specify different traffic restrictions for different VTY lines.

Any router ACL can be configured as a VTY ACL.

This command does not require a license.

Examples

This example shows how to configure VTY ACL to control access to all IPv6 traffic over all VTY lines :

```
switch# configure terminal
switch(config)# ip access-list vtyacl
switch(config-ip-acl)# exit
switch(config)# line vty
switch(config-line)# ipv6 access-class vtyacl1 in
switch(config-line)#
```

This example shows how to remove the VTY ACL from the IPv6 traffic over all VTY lines :

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# no ipv6 access-class vtyacl1 in
switch(config-line)#
```

Related Commands

Command	Description
ip6 access-list	Configures an IPv6 ACL.
show ip6 access-lists	Shows either a specific IPv6 ACL or all IPv4 ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

ipv6 access-class

To apply an IPv6 access control list (ACL) to a virtual terminal (VTY) line, use the **access-class** command. To remove an IPv6 ACL from a VTY line, 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.
in	(Optional) Specifies that the device applies the ACL to inbound traffic.
out	(Optional) Specifies that the device applies the ACL to outbound traffic.

Defaults

None

Command Modes

Line configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to remove dynamically learned, secure MAC addresses from the Ethernet 2/1 interface:

```
switch# config t
switch(config)# line vty
switch(config-line)# ipv6 access-class acl-ipv6-vty01
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.
line	Configures line access to the device.
show ipv6 access-list	Shows all IPv6 ACLs or a specific IPv6 ACL.

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. Names cannot contain a space or quotation mark.

Defaults

No IPv6 ACLs are defined by default.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use IPv6 ACLs to filter IPv6 traffic.

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

Use the **ipv6 traffic-filter** command to apply the ACL to an interface as a router ACL. Use the **ipv6 port traffic-filter** command to apply the ACL to an interface as a port ACL.

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

```
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
deny ipv6 any any
```

Unless you configured an IPv6 ACL with a rule that denies ICMPv6 neighbor discovery messages, the first four rules ensure that the device permits neighbor discovery advertisement and solicitation messages. The fifth rule ensures that the device denies unmatched IPv6 traffic.

Use the **statistics per-entry** command to configure the device to record statistics for each rule in an IPv6 ACL. The device does not record statistics for implicit rules. To record statistics for packets that would match implicit rules, you must explicitly configure an identical rule for each implicit rule.

Note If you explicitly configure an IPv6 ACL with a **deny ipv6 any any** rule, the implicit permit rules can never permit traffic. If you explicitly configure a **deny ipv6 any any** rule but want to permit ICMPv6 neighbor discovery messages, explicitly configure a rule for all five implicit IPv6 ACL rules.

This command does not require a license.

Examples

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

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

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
ipv6 port traffic-filter	Applies an IPv6 ACL to an interface as a port ACL.
ipv6 traffic-filter	Applies an IPv6 ACL to an interface as a router ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
show ipv6 access-lists	Displays all IPv6 ACLs or a specific IPv6 ACL.
statistics per-entry	Enables the collection of statistics for each entry in an ACL.

ipv6 dhcp-ldra

To enable the Lightweight DHCPv6 Relay Agent (LDRA) feature, use the **ipv6 dhcp-ldra** command.

ipv6 dhcp-ldra

no ipv6 dhcp-ldra

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to enable the LDRA feature:

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# ipv6 dhcp-ldra
```

This example shows how to disable the LDRA feature:

```
switch(config)# no ipv6 dhcp-ldra
```

Related Commands

Command	Description
show ipv6 dhcp-ldra	Displays the configuration details of LDRA.

ipv6 dhcp-ldra (interface)

To enable the Lightweight DHCPv6 Relay Agent (LDRA) feature on an interface, use the **ipv6 dhcp-ldra** command.

ipv6 dhcp-ldra {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}

no ipv6 dhcp-ldra {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}

Syntax Description

client-facing-trusted	Specifies client-facing interfaces or ports as trusted.
client-facing-untrusted	Specifies client-facing interfaces or ports as untrusted.
client-facing-disable	Disables LDRA functionality on an interface or port.
server-facing	Specifies an interface or port as server facing.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the LDRA feature by using the **ipv6 dhcp-ldra** command.

Examples

This example shows how to enable the LDRA feature on the specified interface:

```
switch(config)# ipv6 dhcp-ldra
switch(config)# interface ethernet 0/0
switch(config-if)# switchport
switch(config-if)# ipv6 dhcp-ldra client-facing-trusted
```

This example shows how to disable the LDRA feature on the specified interface:

```
switch(config-if)# no ipv6 dhcp-ldra client-facing-trusted
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables the LDRA feature.

ipv6 dhcp-ldra attach-policy vlan

To enable the Lightweight DHCPv6 Relay Agent (LDRA) feature on a VLAN, use the **ipv6 dhcp-ldra attach-policy vlan** command.

ipv6 dhcp-ldra attach-policy vlan *vlan-id* **{client-facing-trusted | client-facing-untrusted}**

no ipv6 dhcp-ldra attach-policy vlan *vlan-id* **{client-facing-trusted | client-facing-untrusted}**

Syntax Description

client-facing-trusted	Specifies client-facing VLAN as trusted.
client-facing-untrusted	Specifies client-facing VLAN as untrusted.
vlan-id	Specifies the VLAN ID.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the LDRA feature by using the **ipv6 dhcp-ldra** command.

Examples

This example shows how to enable the LDRA feature on the specified interface:

```
switch(config)# ipv6 dhcp-ldra
switch(config)# ipv6 dhcp-ldra attach-policy vlan 1032
```

This example shows how to disable the LDRA feature on the specified interface:

```
switch(config)# no ipv6 dhcp-ldra attach-policy vlan 1032
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables the LDRA feature.

ipv6 dhcp relay

To enable the DHCPv6 relay agent, use the **ipv6 dhcp relay** command. To disable the DHCPv6 relay agent, use the **no** form of this command.

ipv6 dhcp relay [**option** {**type cisco** | **vpn**} | **source-interface** *interface*}]

no ipv6 dhcp relay [**option** {**type cisco** | **vpn**} | **source-interface**]

Syntax Description

option	(Optional) Inserts DHCPv6 relay information in relay forward.
type	Specifies the agent option type.
cisco	Specifies Cisco proprietary options.
vpn	Enables DHCPv6 relay agent support across VRFs.
source-interface	Configures the source interface for the DHCPv6 relay.
interface	Source interface. The supported interface types are **ethernet**, **loopback**, **port-channel**, and **VLAN**.

Defaults

DHCPv6 relay agent is enabled by default but **option type cisco** is disabled.

Command Modes

Global configuration

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

You can use the **ipv6 dhcp relay option vpn** command to relay DHCPv6 requests that arrive on an interface in one VRF to a DHCPv6 server in a different VRF.

The **ipv6 dhcp relay option type cisco** command causes the DHCPv6 relay agent to insert virtual subnet selection (VSS) details as part of the vendor-specific option. The **no** option causes the DHCPv6 relay agent to insert VSS details as part of the VSS option (68), which is defined in RFC 6607. This command is useful when you want to use DHCPv6 servers that do not support RFC 6607 but allocate IPv6 addresses based on the client VRF name.

The **ipv6 dhcp relay source-interface** command configures the source interface for the DHCPv6 relay. By default, the DHCPv6 relay agent uses the relay agent address as the source address of the outgoing packet. Configuring the source interface enables you to use a more stable address (such as the loopback interface address) as the source address of relayed messages.

The DHCPv6 relay source interface can be configured globally, per interface, or both. When both the global and interface levels are configured, the interface-level configuration overrides the global configuration.

This command does not require a license.

Examples

This example shows how to enable VRF support for the DHCPv6 relay agent:

```
switch(config)# ipv6 dhcp relay option vpn
```

This example shows how to enable the DHCPv6 relay agent using option type Cisco:

switch(config)# **ipv6 dhcp relay option type cisco**

This example shows how to configure the source interface for the DHCPv6 relay:

switch(config)# **ipv6 dhcp relay option source-interface ethernet 25**

Related Commands

Command	Description
show ipv6 dhcp relay	Displays the DHCPv6 relay configuration.
ipv6 dhcp relay address	Configures an IPv6 address of a DHCPv6 server on an interface.

ipv6 dhcp-ldra

To enable the Lightweight DHCPv6 Relay Agent (LDRA) feature, use the **ipv6 dhcp-ldra** command.

ipv6 dhcp-ldra

no ipv6 dhcp-ldra

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to enable the LDRA feature:

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# ipv6 dhcp-ldra
```

This example shows how to disable the LDRA feature:

```
switch(config)# no ipv6 dhcp-ldra
```

Related Commands

Command	Description
show ipv6 dhcp-ldra	Displays the configuration details of LDRA.

ipv6 dhcp-ldra attach policy (interface)

To enable the Lightweight DHCPv6 Relay Agent (LDRA) feature on an interface, use the **ipv6 dhcp-ldra** command.

ipv6 dhcp-ldra attach-policy {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}

no ipv6 dhcp-ldra attach-policy {client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}

Syntax Description

client-facing-trusted	Specifies client-facing interfaces or ports as trusted.
client-facing-untrusted	Specifies client-facing interfaces or ports as untrusted.
client-facing-disable	Disables LDRA functionality on an interface or port.
server-facing	Specifies an interface or port as server facing.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the LDRA feature by using the **ipv6 dhcp-ldra** command.

Examples

This example shows how to enable the LDRA feature on the specified interface:

```
switch(config)# ipv6 dhcp-ldra
switch(config)# interface ethernet 0/0
switch(config-if)# switchport
switch(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted
```

This example shows how to disable the LDRA feature on the specified interface:

```
switch(config-if)# no ipv6 dhcp-ldra attach-policy client-facing-trusted
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables the LDRA feature.

ipv6 dhcp-ldra attach-policy vlan

To enable the Lightweight DHCPv6 Relay Agent (LDRA) feature on a VLAN, use the **ipv6 dhcp-ldra attach-policy vlan** command.

ipv6 dhcp-ldra attach-policy vlan *vlan-id* **{client-facing-trusted | client-facing-untrusted}**

no ipv6 dhcp-ldra attach-policy vlan *vlan-id* **{client-facing-trusted | client-facing-untrusted}**

Syntax Description

client-facing-trusted	Specifies client-facing VLAN as trusted.
client-facing-untrusted	Specifies client-facing VLAN as untrusted.
vlan-id	Specifies the VLAN ID.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the LDRA feature by using the **ipv6 dhcp-ldra** command.

Examples

This example shows how to enable the LDRA feature on the specified interface:

```
switch(config)# ipv6 dhcp-ldra
switch(config)# ipv6 dhcp-ldra attach-policy vlan 1032 client-facing-trusted
```

This example shows how to disable the LDRA feature on the specified interface:

```
switch(config)# no ipv6 dhcp-ldra attach-policy vlan 1032 client-facing-trusted
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables the LDRA feature.

ipv6 dhcp relay address

To configure the IPv6 address of a DHCPv6 server on an interface, use the **ip dhcp relay address** command. To remove the DHCPv6 server IPv6 address, use the **no** form of this command.

ipv6 dhcp relay address *ipv6-address* [**use-vrf** *vrf-name*] [**interface** *interface*]

no ipv6 dhcp relay address *ipv6-address* [**use-vrf** *vrf-name*] [**interface** *interface*]

Syntax Description

ipv6-address	IPv6 address of the DHCPv6 server.
use-vrf *vrf-name*	Specifies the virtual routing and forwarding (VRF) instance that the DHCPv6 server is in, where the *vrf-name* argument is the name of the VRF. The VRF membership of the interface is connected to the DHCPv6 server that determines the VRF that the DHCP is in.
interface *interface*	Specifies the source interface. The supported interface types are **ethernet**, **port-channel**, and **VLAN**.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

The **ipv6 dhcp relay address** command configures an IPv6 address for a DHCPv6 server to which the relay agent forwards BOOTREQUEST packets received on the configured interface.

Use the **use-vrf** option to specify the VRF name of the server if it is in a different VRF and the other argument interface is used to specify the output interface for the destination.

The server address can either be a link-scoped unicast or multicast address or a global or site-local unicast or multicast address. The **interface** option is mandatory for a link-scoped server address and multicast address. It is not allowed for a global or site-scoped server address.

To configure more than one IP address, use the **ipv6 dhcp relay address** command once per address.

This command does not require a license.

Examples

This example shows how to configure the IPv6 addresses for the DHCPv6 server so that the relay agent can forward BOOTREQUEST packets to the VLAN 25:

```
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 dhcp relay address FF02:1::FF0E:8C6C interface vlan 25
```

Related Commands

Command	Description
ipv6 dhcp relay	Enables or disables the DHCPv6 relay agent.
show ipv6 dhcp relay	Displays the DHCPv6 relay configuration.
show ipv6 dhcp relay statistics	Displays the DHCPv6 relay statistics.

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.

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)	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:

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

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 in the *Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*.

- Layer 3 Ethernet interfaces and subinterfaces
- Layer 3 Ethernet port-channel interfaces and subinterfaces
- Tunnels
- Management interfaces

However, an ACL applied to a Layer 3 interface with the **ipv6 port traffic-filter** command is inactive unless the port mode changes to access or trunk (Layer 2) mode. To apply an IPv6 ACL as a router ACL, use the **ipv6 traffic-filter** command.

You can also apply an IPv6 ACL as a VLAN ACL. For more information, see the **match (VLAN access-map)** command.

The device applies port ACLs to inbound traffic only. The device checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the device continues to process the packet. If the first matching rule denies the packet, the device 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.

If MAC packet classification is enabled on a Layer 2 interface, you cannot use the **ipv6 port traffic-filter** command on the interface.

This command does not require a license.

Examples

This example shows how to apply an IPv6 ACL named ipv6-acl-L2 to Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 port traffic-filter ipv6-acl-L2 in
```

This example shows how to remove an IPv6 ACL named ipv6-acl-L2 from Ethernet interface 1/3:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 port traffic-filter ipv6-acl-L2 in
```

```
switch(config)# show running-config interface ethernet 2/3

!Command: show running-config interface Ethernet2/3
!Time: Wed Jun 24 13:13:48 2009

version 4.2(1)

interface Ethernet2/3
  ip access-group ipacl in
  mac port access-group macacl
  switchport
  mac packet-classify

switch(config)# interface ethernet 2/3
switch(config-if)# ipv6 port traffic-filter v6acl in
ERROR: The given policy cannot be applied as mac packet classification is enable
d on this port
switch(config-if)#
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL.
ipv6 traffic-filter	Applies an IPv6 ACL to an interface as a router ACL.
mac packet-classify	Enables MAC packet classification on a Layer 2 interface.
show access-lists	Displays all ACLs.

Command	Description
show ipv6 access-lists	Shows either a specific IPv6 ACL or all IPv6 ACLs.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.

ipv6 traffic-filter

To apply an IPv6 access control list (ACL) to an interface as a router ACL, 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** | **out**}

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

Syntax Description

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

Defaults

None

Command Modes

Interface configuration

Command History

Release	Modification
4.1(2)	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 as a router 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 in the *Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*.

- Layer 3 Ethernet interfaces and subinterfaces
- Layer 3 Ethernet port-channel interfaces and subinterfaces
- Tunnels
- Management interfaces

You can also use the **ipv6 traffic-filter** command to apply an IPv6 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 **ipv6 traffic-filter** command is inactive unless the port mode changes to routed (Layer 3) mode. To apply an IPv6 ACL as a port ACL, use the **ipv6 port traffic-filter** command.

You can also apply an IPv6 ACL as a VLAN ACL. For more information, see the **match (VLAN access-map)** command.

The device applies router ACLs on either outbound or inbound traffic. When the device applies an ACL to inbound traffic, the device checks inbound packets against the rules in the ACL. If the first matching rule permits the packet, the device continues to process the packet. If the first matching rule denies the packet, the device drops the packet and returns an ICMP host-unreachable message.

For outbound access lists, after receiving and routing a packet to an interface, the device checks the ACL. If the first matching rule permits the packet, the device continues to process the packet. If the first matching rule denies the packet, the device 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.

This command does not require a license.

Examples

This example shows how to apply an IPv6 ACL named ipv6-acl-3A to Ethernet interface 2/1:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ipv6 traffic-filter ipv6-acl-3A in
```

This example shows how to remove an IPv6 ACL named ipv6-acl-3A from Ethernet interface 2/1:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no ipv6 traffic-filter ipv6-acl-3A in
```

Related Commands

Command	Description
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.
show running-config interface	Shows the running configuration of all interfaces or of a specific interface.