



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	<i>policy-name</i>	Name for the identity policy. The name is case sensitive, alphanumeric, and has a maximum of 100 characters.
Defaults	None	
Command Modes	Global configuration	
SupportedUserRoles	network-admin vdc-admin VDC user	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	

Send document comments to nexus7k-docfeedback@cisco.com

Examples

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

```
switch# config t  
switch(config)# identity policy AdminPolicy  
switch(config-id-policy)#
```

This example shows how to remove an identity policy:

```
switch# config t  
switch(config)# no identity policy AdminPolicy
```

Related Commands

Command	Description
show identity policy	Displays identity policy information.

Send document comments to nexus7k-docfeedback@cisco.com

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 eapoudp** command. To remove the EAPoUDP 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

SupportedUserRoles network-admin
vdc-admin
VDC user

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

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

```
switch# config t
switch(config)# no identity profile eapoudp
```

Related Commands	Command	Description
	show identity profile	Displays identity profile information.

Send document comments to nexus7k-docfeedback@cisco.com

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

SupportedUserRoles network-admin
vdc-admin

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

Send document comments to nexus7k-docfeedback@cisco.com

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>access-list-name</i>	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

Supported User Roles

network-admin
vdc-admin

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, Release 4.0*.

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

Send document comments to nexus7k-docfeedback@cisco.com

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.

You can also apply an IPv4 ACL as a VLAN ACL. For more information, see the [match \(VLAN access-map\)](#) command on [page 227](#).

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# config t
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# config t
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>access-list-name</i>	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

Supported User Roles

network-admin
vdc-admin

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.

IPv4 ACLs do not include additional implicit rules to enable the neighbor discovery process. The Address Resolution Protocol (ARP), 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.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

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

```
switch# conf t
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 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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

Supported User Roles network-admin
vdc-admin

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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 <i>number</i> Specifies the buffer size in a range of 0 to 1024 messages.
---------------------------	--

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

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: <pre>switch# configure terminal switch(config)# ip arp inspection log-buffer entries 64 switch(config)#</pre>
-----------------	---

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.

Send document comments to nexus7k-docfeedback@cisco.com

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

Supported User Roles

network-admin
vdc-admin

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	Parameter	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

SupportedUserRoles network-admin
vdc-admin

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.

Send document comments to nexus7k-docfeedback@cisco.com

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	
<i>vlan-list</i>	VLANs on which DAI is active. The <i>vlan-list</i> 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. <ul style="list-style-type: none"> - 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

Supported User Roles network-admin
vdc-admin

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)#
```

Send document comments to nexus7k-docfeedback@cisco.com

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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*

no ip dhcp relay address *IP-address*

Syntax Description	<i>IP-address</i>	IPv4 address of the DHCP server.
---------------------------	-------------------	----------------------------------

Defaults	None
-----------------	------

Command Modes	Interface configuration
----------------------	-------------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.
	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.

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)#
```

Send document comments to nexus7k-docfeedback@cisco.com

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 information option	Enables the insertion and removal of option-82 information from DHCP packets.
ip dhcp snooping	Globally enables DHCP snooping on the device.
service dhcp	Enables or disables the DHCP relay agent.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

Send document comments to nexus7k-docfeedback@cisco.com

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

Supported User Roles

network-admin
vdc-admin

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 address	Configures the IP address of a DHCP server on an interface.
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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
<code>service dhcp</code>	Enables or disables the DHCP relay agent.
<code>show running-config dhcp</code>	Displays DHCP snooping configuration, including IP Source Guard configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

SupportedUserRoles network-admin
vdc-admin

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 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.
	service dhcp	Enables or disables the DHCP relay agent.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

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

Supported User Roles

network-admin
vdc-admin

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.
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.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

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

SupportedUserRoles network-admin
vdc-admin

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)#
```

Send document comments to nexus7k-docfeedback@cisco.com

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.
	show ip dhcp snooping	Displays general information about DHCP snooping.
	show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

SupportedUserRoles network-admin
vdc-admin

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 hardware 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 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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
ip dhcp snooping vlan	Enables DHCP snooping on the specified VLANs.
service dhcp	Enables or disables the DHCP relay agent.
show ip dhcp snooping	Displays general information about DHCP snooping.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>vlan-list</i>	Range of VLANs on which to enable DHCP snooping. The <i>vlan-list</i> 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

SupportedUserRoles network-admin
vdc-admin

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.

Send document comments to nexus7k-docfeedback@cisco.com

Command	Description
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	
<i>access-list-name</i>	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

Supported User Roles

network-admin
vdc-admin

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, Release 4.0*.

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

Send document comments to nexus7k-docfeedback@cisco.com

- 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 on [page 227](#).

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.

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

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.
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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>IP-address</i>	IPv4 address to be used on the specified interface. Valid entries are in dotted-decimal format.
<i>MAC-address</i>	MAC address to be used on the specified interface. Valid entries are in dotted-hexadecimal format.
vlan <i>vlan-id</i>	Specifies the VLAN associated with the IP source entry.
interface ethernet <i>slot/port</i>	Specifies the Layer 2 Ethernet interface associated with the static IP entry.

Defaults

None

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

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)#
```

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com

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

SupportedUserRoles network-admin
vdc-admin

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.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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.

Send document comments to nexus7k-docfeedback@cisco.com

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.

Send document comments to nexus7k-docfeedback@cisco.com