Cisco Nexus 7000 Series Security Command Reference

First Published: --

Last Modified: --

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

CHAPTER 1

CHAPTER 7

CHAPTER 8

CHAPTER 19

CHAPTER 20

Preface

Preface

This preface describes the audience, organization, and conventions of the Book Title. It also provides information on how to obtain related documentation.

This chapter includes the following topics:

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS on Cisco Nexus 7000 Series Platform switches.

Document Conventions

Note

- As part of our constant endeavor to remodel our documents to meet our customers' requirements, we have modified the manner in which we document configuration tasks. As a result of this, you may find a deviation in the style used to describe these tasks, with the newly included sections of the document following the new format.
- The Guidelines and Limitations section contains general guidelines and limitations that are applicable to all the features, and the feature-specific guidelines and limitations that are applicable only to the corresponding feature.

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.

Convention	Description
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

⚠ **Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for Cisco Nexus 7000 Series Switches is available at:

- Configuration Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-and-configuration-guides-list.html

- Command Reference Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-command-reference-list.html

- Release Notes

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-release-notes-list.html

- Install and Upgrade Guides

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-installation-guides-list.html

- Licensing Guide

  http://www.cisco.com/c/en/us/support/switches/nexus-7000-series-switches/products-licensing-information-listing.html

Documentation for Cisco Nexus 7000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders is available at the following URL:

http://www.cisco.com/c/en/us/support/switches/nexus-2000-series-fabric-extenders/products-installation-and-configuration-guides-list.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus7k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

A Commands

absolute

To specify a time range that has a specific start date and time, a specific end date and time, or both, use the **absolute** command. To remove an absolute time range, use the **no** form of this command.

[*sequence-number*] **absolute** [**start** *time date*] [**end** *time date*]

no {*sequence-number*| **absolute** [**start** *time date*] [**end** *time date*]}

Syntax Description

sequence-number	(Optional) Sequence number of the rule, which causes the device to insert the command in that numbered position in the time range. Sequence numbers maintain the order of rules within a time range. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in a time range has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the time range and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
start *time date*	(Optional) Specifies the exact time and date when the device begins enforcing the **permit** and **deny** rules associated with the time range. If you do not specify a start time and date, the device enforces the **permit** or **deny** rules immediately. For information about value values for the *time* and *date* arguments, see the “Usage Guidelines” section.
end *time date*	(Optional) Specifies the exact time and date when the device stops enforcing the **permit** and **deny** commands associated with the time range. If you do not specify an end time and date, the device always enforces the **permit** or **deny** rules after the start time and date have passed. For information about the values for the *time* and *date* arguments, see the “Usage Guidelines” section.

Command Default

None

Command Modes

Time-range configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The device interprets all time range rules as local time.

If you omit both the **start** and the **end** keywords, the device considers the absolute time range to be always active.

You specify *time* arguments in 24-hour notation, in the form of *hours*:*minutes* or *hours*:*minutes*:*seconds*. For example, in 24-hour notation, 8:00 a.m. is 8:00 and 8:00 p.m. is 20:00.

You specify *date* arguments in the *day month year* format. The minimum valid start time and date is 00:00:00 1 January 1970, and the maximum valid start time is 23:59:59 31 December 2037.

This command does not require a license.

Examples

This example shows how to create an absolute time rule that begins at 7:00 a.m. on September 17, 2007, and ends at 11:59:59 p.m. on September 19, 2007:

```
switch# configure terminal
switch(config)# time-range conference-remote-access
switch(config-time-range)# absolute start 07:00 17 September 2007 end 23:59:59 19 September
 2007
```

Related Commands

Command	Description
periodic	Configures a periodic time range rule.
time-range	Configures a time range for use in IPv4 or IPv6 ACLs.

accept-lifetime

To specify the time interval within which the device accepts a key during a key exchange with another device, use the **accept-lifetime** command. To remove the time interval, use the **no** form of this command.

accept-lifetime [local] *start-time* [**duration** *duration-value*| **infinite**| *end-time*]

no accept-lifetime [local] *start-time* [**duration** *duration-value*| **infinite**| *end-time*]

Syntax Description

local	(Optional) Specifies that the device treats the configured times as local times. By default, the device treats the *start-time* and *end-time* arguments as UTC.
start-time	Time of day and date that the device begins accepting the key. For information about the values for the *start-time* argument, see the “Usage Guidelines” section.
duration *duration-value*	(Optional) Specifies the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).
infinite	(Optional) Specifies that the key never expires.
end-time	(Optional) Time of day and date that the device stops accepting the key. For information about the values for the *time of day* and *date* arguments, see the “Usage Guidelines” section.

Command Default

infinite

Command Modes

Key configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

By default, the device interprets all time range rules as UTC.

By default, the time interval within which the device accepts a key during a key exchange with another device—the accept lifetime—is infinite, which means that the key is always valid.

The *start-time* and *end-time* arguments both require time and date components, in the following format:

hour[:*minute*[:*second*]] *month day year*

You specify the hour in 24-hour notation. For example, in 24-hour notation, 8:00 a.m. is 8:00 and 8:00 p.m. is 20:00. The minimum valid *start-time* is 00:00:00 Jan 1 1970, and the maximum valid *start-time* is 23:59:59 Dec 31 2037.

This command does not require a license.

Examples

This example shows how to create an accept lifetime that begins at midnight on June 13, 2008, and ends at 11:59:59 p.m. on August 12, 2008:

```
switch# configure terminal

switch(config)# key chain glbp-keys

switch(config-keychain)# key 13

switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2008 23:59:59 Sep 12 2008

switch(config-keychain-key)#
```

Related Commands

Command	Description
key	Configures a key.
keychain	Configures a keychain.
key-string	Configures a key string.
send-lifetime	Configures a send lifetime for a key.
show key chain	Shows keychain configuration.

access-class

To apply an IPv4 access control list (ACL) to a virtual terminal (VTY) line, use the **access-class** command. To remove an IPv4 ACL from a VTY line, use the **no** form of this command.

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

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

Syntax Description

access-list-name	Name of the IPv4 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.

Command Default

None

Command Modes

Line configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Because a user can connect to any VTY line, you should set identical restrictions on all virtual terminal lines.

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)# clear port-security dynamic interface ethernet 2/1
```

This example shows how to remove the dynamically learned, secure MAC addresses 0019.D2D0.00AE:

```
switch# config t
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

Related Commands

Command	Description
ip access-list	Provides debugging information for port security.
line	Enables port security globally.
show line	Shows information about port security.

action

To specify what the device does when a packet matches a **permit** command in a VLAN access control list (VACL), use the **action** command. To remove an **action** command, use the **no** form of this command.

action drop [log]

no action drop [log]

action forward

no action forward

action redirect{**ethernet** *slot* **|** *port* | **port-channel** *channel-number.subinterface-number*}

no action redirect{**ethernet** *slot* **|** *port* | **port-channel** *channel-number.subinterface-number*}

Syntax Description

drop	Specifies that the device drops the packet.
log	(Optional) Specifies that the device logs the packets it drops because of the **drop** keyword.
forward	Specifies that the device forwards the packet to its destination port.
redirect	Specifies that the device redirects the packet to an interface.
ethernet *slot*/*port*	Specifies the Ethernet interface that the device redirects the packet to.
port-channel *channel-number***.***subinterface-number*	Specifies the port-channel interface that the device redirects the packet to. **Note** The dot separator is required between the *channel-number* and *subinterface-number* arguments.

Command Default

None

Command Modes

VLAN access-map configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **action** command specifies the action that the device takes when a packet matches the conditions in an ACL specified by a **match** command in the same access map entry as the **action** command.

This command does not require a license.

Examples

This example shows how to create a VLAN access map named vlan-map-01 and add two entries that each have two **match** commands and one **action** command:

```
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# match mac address mac-acl-00f
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-320
switch(config-access-map)# match mac address mac-acl-00e
switch(config-access-map)# action drop
switch(config-access-map)# show vlan access-map
Vlan access-map vlan-map-01 10
        match ip: ip-acl-01
        match mac: mac-acl-00f
        action: forward
Vlan access-map vlan-map-01 20
        match ip: ip-acl-320
        match mac: mac-acl-00e
        action: drop
```

Related Commands

Command	Description
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
statistics	Enables statistics for an access control list or VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

arp access-list

To create an Address Resolution Protocol (ARP) access control list (ACL) or to enter ARP access list configuration mode for a specific ARP ACL, use the **arp access-list** command. To remove an ARP ACL, use the **no** form of this command.

arp access-list *access-list-name*

no arp access-list *access-list-name*

Syntax Description

access-list-name	Name of the ARP ACL. The name can be up to 64 alphanumeric, case-sensitive characters. Names cannot contain a space or quotation mark.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use ARP ACLs to filter ARP traffic when you cannot use DCHP snooping.

No ARP ACLs are defined by default.

When you use the **arp access-list** command, the device enters ARP access list configuration mode, where you can use the ARP **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 arp inspection filter** command to apply the ARP ACL to a VLAN.

This command does not require a license.

Examples

This example shows how to enter ARP access list configuration mode for an ARP ACL named arp-acl-01:

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)#
```

Related Commands

Command	Description
deny (ARP)	Configures a deny rule in an ARP ACL.
ip arp inspection filter	Applies an ARP ACL to a VLAN.
permit (ARP)	Configures a permit rule in an ARP ACL.
show arp access-lists	Displays all ARP ACLs or a specific ARP ACL.

authentication (LDAP)

To configure Lightweight Directory Access Protocol (LDAP) authentication to use the bind or compare method, use the **authentication** command. To disable this configuration, use the **no** form of this command.

authentication {**bind-first** [**append-with-baseDN DNstring**]| **compare** [**password-attribute password**]}

no authentication {**bind-first** [**append-with-baseDN DNstring**]| **compare** [**password-attribute password**]}

Syntax Description

bind-first	Sets the LDAP authentication method to bind first.
append-with-baseDN *DNstring*	(Optional) Specifies the designated name (DN) string. You can enter up to 63 alphanumeric characters.
compare	Sets the LDAP authentication method to compare.
password-attribute *password*	(Optional) Specifies the user password. You can enter up to 63 alphanumeric characters.

Command Default

Bind method using first search and then bind

Command Modes

LDAP server group 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 configure LDAP authentication to use the compare method:

```
switch# conf t
switch(config)# aaa group server ldap LDAPServer1
switch(config-ldap)# server 10.10.2.2
switch(config-ldap)# authentication compare password-attribute TyuL8r
switch(config-ldap)#
```

Related Commands

Command	Description
aaa group server ldap	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.

Command	Description
server	Configures the LDAP server as a member of the LDAP server group.
show ldap-server groups	Displays the LDAP server group configuration.

aaa accounting default

To configure authentication, authorization, and accounting (AAA) methods for accounting, use the **aaa accounting default** command. To revert to the default, use the **no** form of this command.

aaa accounting default {**group group-list**| **local**}

no aaa accounting default {**group group-list**| **local**}

Syntax Description

group	Specifies to use a server group for accounting.
group-list	Space-separated list of server groups that can include the following: • **radius** for all configured RADIUS servers. • Any configured RADIUS or TACACS+ server group name. The maximum number of names in the list is eight.
local	Specifies to use the local database for accounting.

Command Default

local

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **group** *group-list* methods refer to a set of previously defined servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the RADIUS server groups on the device.

If you specify the **group** method, the **local** method, or both, and they fail, then the accounting authentication fails.

If you specify more that one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Examples

This example shows how to configure any RADIUS server for AAA accounting:

```
switch# configure terminal
switch(config)# aaa accounting default group radius
```

Related Commands

Command	Description
aaa group server	Configures AAA RADIUS server groups.
radius-server host	Configures RADIUS servers.
show aaa accounting	Displays AAA accounting status information.
show aaa groups	Displays AAA server group information.
tacacs-server host	Configures TACACS+ servers.

aaa accounting dot1x

To configure authentication, authorization, and accounting (AAA) methods for accounting for 802.1X authentication, use the **aaa accounting dot1x** command. To revert to the default, use the **no** form of this command.

aaa accounting dot1x {**group group-list**| **local**}

no aaa accounting dot1x {**group group-list**| **local**}

Syntax Description

group	Specifies to use a server group for accounting.
group-list	Space-separated list of RADIUS server groups that can include the following: • **radius** for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.
local	Specifies to use the local database for accounting.

Command Default

local

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **group** *group-list* methods refer to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the RADIUS server groups on the device.

If you specify the **group** method, the **local** method, or both, and they fail, then the accounting authentication fails.

If you specify more that one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Examples

This example shows how to configure authentication, authorization, and accounting (AAA) methods for accounting for 802.1X authentication:

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group group-list
```

Related Commands

Command	Description
aaa group server radius	Configures AAA RADIUS server groups.
radius-server host	Configures RADIUS servers.
show aaa accounting	Displays AAA accounting status information.
show aaa groups	Displays AAA server group information.

aaa authentication cts default group

To configure the default authentication, authorization, and accounting (AAA) RADIUS server groups for Cisco TrustSec authentication, use the **aaa authentication cts default group** command. To remove a server group from the default AAA authentication server group list, use the **no** form of this command.

aaa authentication cts default group *group-list*

no aaa authentication cts default group *group-list*

Syntax Description

group-list	Space-separated list of RADIUS server groups that can include the following: • **radius** for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.

Command Default

None

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 Cisco TrustSec feature using the **feature cts** command.

The *group-list* refers to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the RADIUS server groups on the device.

If you specify more that one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

This command requires the Advanced Services license.

Examples

This example shows how to configure the default AAA authentication RADIUS server group for Cisco TrustSec:

```
switch# configure terminal
swtich(config)# aaa authentication cts default group RadGroup
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature cts	Enables the Cisco TrustSec feature.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays the AAA authentication configuration.
show aaa groups	Displays the AAA server groups.

aaa authentication dot1x default group

To configure AAA authentication methods for 802.1X, use the **aaa authentication dot1x default group** command. To revert to the default, use the **no** form of this command.

aaa authentication dot1x default group *group-list*

no aaa authentication dot1x default group *group-list*

Syntax Description

group-list	Space-separated list of RADIUS server groups that can include the following: • **radius** for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

The *group-list* refers to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the RADIUS server groups on the device.

If you specify more that one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Examples

This example shows how to configure methods for 802.1X authentication:

```
switch# configure terminal
switch(config)# aaa authentication do1x default group Dot1xGroup
```

This example shows how to revert to the default methods for 802.1X authentication:

```
switch# configure terminal
switch(config)# no aaa authentication do1x default group Dot1xGroup
```

Related Commands

Command	Description
feature dot1x	Enables 802.1X.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays the AAA authentication configuration.
show aaa groups	Displays the AAA server groups.

aaa authentication eou default group

To configure AAA authentication methods for EAP over UDP (EoU), use the **aaa authentication eou default group** command. To revert to the default, use the **no** form of this command.

aaa authentication eou default group *group-list*

no aaa authentication eou default group *group-list*

Syntax Description

group-list	Space-separated list of RADIUS server groups that can include the following: • **radius** for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Before configuring EAPoUDP default authentication methods, you must enable EAPoUDP using the **feature eou** command.

The *group-list* refers to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the RADIUS server groups on the device.

If you specify more that one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

This command does not require a license.

Examples

This example shows how to configure methods for EAPoUDP authentication:

```
switch# configure terminal
switch(config)# aaa authentication eou default group EoUGroup
```

This example shows how to revert to the default methods for EAPoUDP authentication:

```
switch# configure terminal
switch(config)# no aaa authentication eou default group EoUGroup
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays the AAA authentication configuration.
show aaa groups	Displays the AAA server groups.

aaa authentication login ascii-authentication

To enable ASCII authentication for passwords on a TACACS+ server, use the aaa authentication login ascii-authentication command. To revert to the default, use the no form of this command.

aaa authentication login ascii-authentication

no aaa authentication login ascii-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Only the TACACS+ protocol supports this feature.

This command does not require a license.

Examples

This example shows how to enable ASCII authentication for passwords on TACACS+ servers:

```
switch# configure terminal
switch(config)# aaa authentication login ascii-authentication
```

This example shows how to disable ASCII authentication for passwords on TACACS+ servers:

```
switch# configure terminal
switch(config)# no aaa authentication login ascii-authentication
```

Related Commands

Command	Description
show aaa authentication login ascii-authentication	Displays the status of the ASCII authentication for passwords.

aaa authentication login chap enable

To enable Challenge Handshake Authentication Protocol (CHAP) authentication at login, use the **aaa authentication login chap enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login chap enable

no aaa authentication login chap enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You cannot enable both CHAP and MSCHAP or MSCHAP V2 on your Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable CHAP authentication:

```
switch# configure terminal
switch(config)# aaa authentication login chap enable
```

This example shows how to disable CHAP authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login chap enable
```

Related Commands

Command	Description
show aaa authentication login chap	Displays the status of CHAP authentication.

aaa authentication login console

To configure AAA authentication methods for console logins, use the **aaa authentication login console** command. To revert to the default, use the **no** form of this command.

aaa authentication login console {**fallback error local**| **group** *group-list* **[none]**| **local**| **none**}

no aaa authentication login console {**fallback error local**| **group** *group-list* **[none]**| **local**| **none**}

Syntax Description

fallback error local	Enables fallback to local authentication for the console login if remote authentication is configured and all AAA servers are unreachable. Fallback to local authentication is enabled by default. **Note** Disabling fallback to local authentication can lock your Cisco NX-OS device, forcing you to perform a password recovery in order to gain access. To prevent being locked out of the device, we recommend disabling fallback to local authentication for only the default login or the console login, not both.
group	Specifies to use a server group for authentication.
group-list	Space-separated list of server groups. The list can include the following: • **radius** for all configured RADIUS servers. • **tacacs+** for all configured TACACS+ servers. • **ldap** for all configured LDAP servers. • Any configured RADIUS, TACACS+, or LDAP server group name.
none	(Optional) Specifies that no authentication is to be used.
local	Specifies to use the local database for authentication.

Command Default

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	Support for LDAP server groups was added.
5.0(2)	The **fallback error local** keyword was added**.**
4.0(1)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, **group ldap,** and **group** *group-list* methods refer to a set of previously defined RADIUS, TACACS+, or LDAP servers. Use the **radius-server host, tacacs-server host, or ldap-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the server groups on the device.

If you specify more that one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

If you specify the **group** method or **local** method and they fail, the authentication can fail. If you specify the **none** method alone or after the **group** method, the authentication always succeeds.

The command operates only in the default VDC (VDC 1).

This command does not require a license.

Examples

This example shows how to configure the AAA authentication console login methods:

```
switch# configure terminal
switch(config)# aaa authentication login console group radius
```

This example shows how to revert to the default AAA authentication console login method:

```
switch# configure terminal
switch(config)# no aaa authentication login console group radius
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
ldap-server host	Configures LDAP servers.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays AAA authentication information.
show aaa groups	Displays the AAA server groups.
tacacs-server host	Configures TACACS+ servers.

aaa authentication login default

To configure the default AAA authentication methods, use the **aaa authentication login default** command. To revert to the default, use the **no** form of this command.

aaa authentication login default {**fallback error local**| **group** *group-list* **[none]**| **local**| **none**}

no aaa authentication login default {**fallback error local**| **group** *group-list* **[none]**| **local**| **none**}

Syntax Description

fallback error local	Enables fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable. Fallback to local authentication is enabled by default. **Note** Disabling fallback to local authentication can lock your Cisco NX-OS device, forcing you to perform a password recovery in order to gain access. To prevent being locked out of the device, we recommend disabling fallback to local authentication for only the default login or the console login, not both.
group	Specifies a server group list to be used for authentication.
group-list	Space-separated list of server groups that can include the following: • **radius** for all configured RADIUS servers. • **tacacs+** for all configured TACACS+ servers. • **ldap** for all configured LDAP servers. • Any configured RADIUS, TACACS+, or LDAP server group name.
none	(Optional) Specifies that no authentication is to be used.
local	Specifies to use the local database for authentication.

Command Default

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	Support for LDAP server groups was added.
5.0(2)	The **fallback error local** keyword was added**.**
4.0(1)	This command was introduced.

Usage Guidelines

The **group radius, group tacacs+**, **group ldap**, and **group** *group-list* methods refer to a set of previously defined RADIUS, TACACS+, or LDAP servers. Use the **radius-server host, tacacs-server host**, or **ldap-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the server groups on the device.

If you specify more that one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

If you specify the **group** method or **local** method and they fail, the authentication fails. If you specify the **none** method alone or after the **group** method, the authentication always succeeds.

This command does not require a license.

Examples

This example shows how to configure the AAA authentication default login method:

```
switch# configure terminal
switch(config)# aaa authentication login default group radius
```

This example shows how to revert to the default AAA authentication default login method:

```
switch# configure terminal
switch(config)# no aaa authentication login default group radius
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
ldap-server host	Configures LDAP servers.
radius-server host	Configures RADIUS servers.
show aaa authentication	Displays AAA authentication information.
show aaa groups	Displays the AAA server groups.
tacacs-server host	Configures TACACS+ servers.

aaa authentication login error-enable

To configure that the AAA authentication failure message displays on the console, use the **aaa authentication login error-enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login error-enable

no aaa authentication login error-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When you log in, the login is processed by rolling over to the local user database if the remote AAA servers do not respond. In such cases, the following message is displayed on the user's terminal—if you have enabled the displaying of login failure messages:

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

This command does not require a license.

Examples

This example shows how to enable the display of AAA authentication failure messages to the console:

```
switch# configure terminal
switch(config)# aaa authentication login error-enable
```

This example shows how to disable the display of AAA authentication failure messages to the console:

```
switch# configure terminal
switch(config)# no aaa authentication login error-enable
```

Related Commands

Command	Description
show aaa authentication login error-enable	Displays the status of the AAA authentication failure message display.

aaa authentication login invalid-username-log

To include the username in authentication failed messages for all failure reasons, use the **aaa authentication login invalid-username-log** command. To revert to the default, use the **no** form of this command. This applies to both local and remote authentication.

aaa authentication login invalid-username-log

show aaa authentication login invalid-username-log

no aaa authentication login invalid-username-log

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

It is a Configuration Mode Command

Command History

Release	Modification
7.1	This Command was introduced.

Usage Guidelines

The above command will cause the username to be included in authentication failed messages for all failure reasons. This is irrespective of whether the username is valid or not since under some conditions the switch cannot determine a username's validity. This applies to both local and remote authentication.

This command does not require a license.

Examples

This example shows how to include the username in authentication failed messages for all failure reasons:

```
switch# configure terminal
switch(config)# aaa authentication login invalid-username-log
```

This example shows how to exclude the username in authentication failed messages for all failure reasons:

```
switch# configure terminal
switch(config)# no aaa authentication login invalid-username-log
```

aaa authentication login mschap enable

To enable Microsoft Challenge Handshake Authentication Protocol (MSCHAP) authentication at login, use the **aaa authentication login mschap enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login mschap enable

no aaa authentication login mschap enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You cannot enable both MSCHAP and CHAP or MSCHAP V2 on your Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable MSCHAP authentication:

```
switch# configure terminal
switch(config)# aaa authentication login mschap enable
```

This example shows how to disable MSCHAP authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login mschap enable
```

Related Commands

Command	Description
show aaa authentication login mschap	Displays the status of MSCHAP authentication.

aaa authentication login mschapv2 enable

To enable Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) authentication at login, use the **aaa authentication login mschapv2 enable** command. To revert to the default, use the **no** form of this command.

aaa authentication login mschapv2 enable

no aaa authentication login mschapv2 enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You cannot enable both MSCHAP V2 and CHAP or MSCHAP on your Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable MSCHAP V2 authentication:

```
switch# configure terminal
switch(config)# aaa authentication login mschapv2 enable
```

This example shows how to disable MSCHAP V2 authentication:

```
switch# configure terminal
switch(config)# no aaa authentication login mschapv2 enable
```

Related Commands

Command	Description
show aaa authentication login mschapv2	Displays the status of MSCHAP V2 authentication.

aaa authentication rejected

To configure the login block per user, use the **aaa authentication rejected** command. To remove the login block per user, use the **no** form of this command.

aaa authentication rejected *attempts* **in** *seconds* **ban** *block-seconds*

no aaa authentication rejected

Syntax Description

attempts	Number of login attempts fail before a user is blocked.
seconds	Time period within which the login attempt fails.
block-seconds	Time period in which the user is blocked after a failed login attempt.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

This feature is applicable only for local users.

Examples

The following example shows how to configure the login parameters to block a user for 300 seconds when 5 login attempts fail within a period of 60 seconds.

```
switch# configure terminal
swtich(config)# aaa authentication rejected 5 in 60 ban 300
```

Related Commands

Command	Description
clear aaa local user blocked	Clears the blocked local user.
show aaa authentication	Displays the AAA authentication configuration.
show aaa local user blocked	Displays the blocked local users.

aaa authorization commands default

To configure default AAA authorization methods for all EXEC commands, use the **aaa authorization commands default** command. To revert to the default, use the **no** form of this command.

aaa authorization commands default [**group** *group-list* [**local**]| **local**]

no aaa authorization commands default [**group** *group-list* [**local**]| **local**]

Syntax Description

group	(Optional) Specifies to use a server group for authorization.
group-list	Space-separated list of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • Any configured TACACS+ server group name.
local	(Optional) Specifies to use the local role-based database for authentication.

Command Default

Local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	The **none** keyword was deprecated.
4.2(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature using the **feature tacacs+** command.

The **group tacacs+** and **group** *group-list* methods refer to a set of previously defined TACACS+ servers. Use the **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers. Use the **show aaa groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, then the authorization can fail. If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond.

Caution Command authorization disables user role based authorization control (RBAC), including the default roles.

Note Command authorization is available only to non-console sessions. If you use a console to login to the server, command authorization is disabled.

Note By default, context sensitive help and command tab completion show only the commands supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

This command does not require a license.

Examples

This example shows how to configure the default AAA authorization methods for EXEC commands:

```
switch# configure terminal
switch(config)# aaa authorization commands default group TacGroup local
Per command authorization will disable RBAC for all users. Proceed (y/n)?
```

Note If you press **Enter** at the confirmation prompt, the default response is **n**.

This example shows how to revert to the default AAA authorization methods for EXEC commands:

```
switch# configure terminal
switch(config)# no aaa authorization commands default group TacGroup local
```

Related Commands

Command	Description
aaa authorization config-commands default	Configures default AAA authorization methods for configuration commands.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.
terminal verify-only	Enables the command authorization verification.
test aaa authorization command-type	Tests the command authorization using the AAA command authorization methods.

aaa authorization config-commands default

To configure default AAA authorization methods for all configuration commands, use the **aaa authorization config-commands default** command. To revert to the default, use the **no** form of this command.

aaa authorization config-commands default [**group** *group-list* **[local]|** **local**]

no aaa authorization config-commands default [**group** *group-list* **[local]|** **local**]

Syntax Description

group	(Optional) Specifies to use a server group for authorization.
group-list	Space-separated list of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • Any configured TACACS+ server group name.
local	(Optional) Specifies to use the local role-based database for authentication.

Command Default

Local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	The **none** keyword was deprecated.
4.2(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature using the **feature tacacs+** command.

The **group tacacs+** and **group** *group-list* methods refer to a set of previously defined TACACS+ servers. Use the **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers. Use the **show aaa groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, then the authorization can fail. If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond.

Caution Command authorization disables user role based authorization control (RBAC), including the default roles.

Note Command authorization is available only to non-console sessions. If you use a console to login to the server, command authorization is disabled.

Note By default, context sensitive help and command tab completion show only the commands supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

This command does not require a license.

Examples

This example shows how to configure the default AAA authorization methods for configuration commands:

```
switch# configure terminal
switch(config)# aaa authorization config-commands default group TacGroup local
```

This example shows how to revert to the default AAA authorization methods for configuration commands:

```
switch# configure terminal
switch(config)# no aaa authorization config-commands default group TacGroup local
```

Related Commands

Command	Description
aaa authorization commands default	Configures default AAA authorization methods for EXEC commands.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.
terminal verify-only	Enables the command authorization verification.
test aaa authorization command-type	Tests the command authorization using the AAA command authorization methods.

aaa authorization cts default group

To configure the default authentication, authorization, and accounting (AAA) RADIUS server groups for Cisco TrustSec authorization, use the **aaa authorization cts default group** command. To remove a server group from the default AAA authorization server group list, use the **no** form of this command.

aaa authorization cts default group *group-list*

no aaa authorization cts default group *group-list*

Syntax Description

group-list	Space-separated list of RADIUS server groups that can include the following: • **radius** for all configured RADIUS servers. • Any configured RADIUS server group name. The maximum number of names in the list is eight.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use the **aaa authorization cts default group** command, you must enable the Cisco TrustSec feature using the **feature cts** command.

The *group-list* refers to a set of previously defined RADIUS servers. Use the **radius-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa groups** command to display the RADIUS server groups on the device.

If you specify more that one server group, the Cisco NX-OS software checks each group in the order that you specify in the list.

This command requires the Advanced Services license.

Examples

This example shows how to configure the default AAA authorization RADIUS server group for Cisco TrustSec:

```
switch# configure terminal
switch(config)# aaa authorization cts default group RadGroup
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show aaa authorization	Displays the AAA authorization configuration.
show aaa groups	Displays the AAA server groups.

aaa authorization ssh-certificate

To configure the default AAA authorization method for TACACS+ or Lightweight Directory Access Protocol (LDAP) servers, use the **aaa authorization ssh-certificate** command. To disable this configuration, use the **no** form of this command.

aaa authorization ssh-certificate default {**group** *group-list*| **local**}

no aaa authorization ssh-certificate default {**group** *group-list*| **local**}

Syntax Description

group	Specifies to use a server group for authorization.
group-list	Space-separated list of server groups. The list can include the following: • **tacacs+** for all configured TACACS+ servers. • **ldap** for all configured LDAP servers. • Any configured TACACS+ or LDAP server group name.
local	Specifies to use the local database for authentication.

Command Default

local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the TACACS+ feature using the **feature tacacs+** command or the LDAP feature using the **feature ldap** command.

The **group tacacs+**, **group ldap**, and **group** *group-list* methods refer to a set of previously defined TACACS+ and LDAP servers. Use the **tacacs-server host** command or **ldap-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers. Use the **show aaa groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, the authorization can fail. If you have not configured a fallback method after the TACACS+ or LDAP server group method, authorization fails if all server groups fail to respond.

This command does not require a license.

Examples

This example shows how to configure LDAP authorization with certificate authentication as the default AAA authorization method for LDAP servers:

```
switch# configure terminal
switch(config)# aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
```

Related Commands

Command	Description
aaa authorization ssh-publickey	Configures LDAP or local authorization with the SSH public key as the default AAA authorization method for LDAP servers.
feature ldap	Enables the LDAP feature.
feature tacacs+	Enables the TACACS+ feature.
show aaa authorization	Displays the AAA authorization configuration.

aaa authorization ssh-publickey

To configure Lightweight Directory Access Protocol (LDAP) or local authorization with the Secure Shell (SSH) public key as the default AAA authorization method for LDAP servers, use the **aaa authorization ssh-publickey** command. To revert to the default, use the **no** form of this command.

aaa authorization ssh-publickey default {**group** *group-list*| **local**}

no aaa authorization ssh-publickey default {**group** *group-list*| **local**}

Syntax Description

group	Specifies to use a server group for authorization.
group-list	Space-separated list of server groups. The list can include the following: • **ldap** for all configured LDAP servers. • Any configured LDAP server group name.
local	Specifies to use the local database for authentication.

Command Default

Local

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the LDAP feature using the **feature ldap** command.

The **group ldap** and **group** *group-list* methods refer to a set of previously defined LDAP servers. Use the **ldap-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers. Use the **show aaa groups** command to display the server groups on the device.

If you specify more than one server group, the Cisco NX-OS software checks each group in the order that you specify in the list. The **local** method is used only if all the configured server groups fail to respond and you have configured **local** as the fallback method.

If you specify the **group** method or **local** method and it fails, the authorization can fail. If you have not configured a fallback method after the LDAP server group method, authorization fails if all server groups fail to respond.

This command does not require a license.

Examples

This example shows how to configure LDAP authorization with the SSH public key as the default AAA authorization method for LDAP servers:

```
switch# configure terminal
switch(config)# aaa authorization ssh-publickey default group LDAPServer1 LDAPServer2
```

Related Commands

Command	Description
aaa authorization ssh-certificate	Configures LDAP or local authorization with certificate authentication as the default AAA authorization method for LDAP servers.
feature ldap	Enables the LDAP feature.
show aaa authorization	Displays the AAA authorization configuration.

aaa group server ldap

To create a Lightweight Directory Access Protocol (LDAP) server group and enter LDAP server group configuration mode , use the **aaa group server ldap** command. To delete an LDAP server group, use the **no** form of this command.

aaa group server ldap *group-name*

no aaa group server ldap *group-name*

Syntax Description

group-name	LDAP server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Command Default

None

Command Modes

Global configuration

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you configure LDAP.

This command does not require a license.

Examples

This example shows how to create an LDAP server group and enter LDAP server configuration mode:

```
switch# configure terminal
switch(config)# aaa group server ldap LdapServer
switch(config-ldap)#
```

This example shows how to delete an LDAP server group:

```
switch# configure terminal
switch(config)# no aaa group server ldap LdapServer
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show aaa groups	Displays server group information.

aaa group server radius

To create a RADIUS server group and enter RADIUS server group configuration mode , use the **aaa group server radius** command. To delete a RADIUS server group, use the **no** form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

Syntax Description

group-name	RADIUS server group name.The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Command Default

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 a RADIUS server group and enter RADIUS server configuration mode:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

This example shows how to delete a RADIUS server group:

```
switch# configure terminal
switch(config)# no aaa group server radius RadServer
```

Related Commands

Command	Description
show aaa groups	Displays server group information.

aaa group server tacacs+

To create a TACACS+ server group and enter TACACS+ server group configuration mode , use the **aaa group server tacacs+** command. To delete a TACACS+ server group, use the **no** form of this command.

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Syntax Description

group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	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 create a TACACS+ server group and enter TACACS+ server configuration mode:

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-radius)#
```

This example shows how to delete a TACACS+ server group:

```
switch# configure terminal
switch(config)# no aaa group server tacacs+ TacServer
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show aaa groups	Displays server group information.

aaa user default-role

To allow remote users who do not have a user role to log in to the device through RADIUS or TACACS+ using a default user role, use the **aaa user default-role** command. To disable default user roles for remote users, use the **no** form of this command.

aaa user default-role

no aaa user default-role

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

You can enable or disable this feature for the virtual device context (VDC) as needed. For the default VDC, the default role is network-operator. For nondefault VDCs, the default VDC is vdc-operator. When you disable the AAA default user role feature, remote users who do not have a user role cannot log in to the device.

This command does not require a license.

Examples

This example shows how to enable default user roles for AAA authentication of remote users:

```
switch# configure terminal
switch(config)# aaa user default-role
```

This example shows how to disable default user roles for AAA authentication of remote users:

```
switch# configure terminal
switch(config)# no aaa user default-role
```

Related Commands

Command	Description
show aaa user default-role	Displays the status of AAA default user role feature.

C Commands

cipher suite

To configure a cipher suite for encrypting traffic with MACsec, use the **cipher suite** command. To reset the cipher suite to its default value, use the **no** form of this command.

cipher suite {**GCM-AES-128** | **GCM-AES-256** | **GCM-AES-XPN-128** | **GCM-AES-XPN-256**}

no cipher suite {**GCM-AES-128** | **GCM-AES-256** | **GCM-AES-XPN-128** | **GCM-AES-XPN-256**}

Syntax Description

GCM-AES-128	Specifies the Galois/Counter Mode (GCM) encryption method, Advanced Encryption Standard (AES) encryption algorithm, and 128-bit encryption.
GCM-AES-256	Specifies the GCM encryption method, AES encryption algorithm, and 256-bit encryption.
GCM-AES-XPN-128	Specifies the GCM encryption method, AES encryption algorithm that uses Extended Packet Numbering (XPN) of 64 bits, and 128-bit encryption.
GCM-AES-XPN-256	Specifies the GCM encryption method, AES encryption algorithm that uses Extended Packet Numbering (XPN) of 64 bits, and 256-bit encryption.

[1]

Command Default

The default cipher suite chosen for encryption is GCM-AES-XPN-256.

Command Modes

MACsec policy configuration (config-macsec-policy)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, you should enable the MACsec Key Agreement (MKA) feature first.

[1]
- GCM indicates the encryption method.
- AES and AES-XPN indicates the hash or integrity algorithm.
- The numeral indicates the length of the cipher.

Examples

This example shows how to configure a cipher suite:

```
switch# configure terminal
switch(config)# macsec policy p1
switch(config-macsec-policy)# cipher suite GCM-AES-XPN-128
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
macsec keychain policy	Configures a MACsec keychain policy.
macsec policy	Configures a MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

clear access-list counters

To clear the counters for all IPv4, IPv6, and MAC access control lists (ACLs) or a single ACL, use the **clear access-list counters** command.

clear access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(2)	Added support for clearing IPv6 ACL counters.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear counters for all IPv4, IPv6, and MAC ACLs:

```
switch# clear access-list counters
switch#
```

This example shows how to clear counters for an IPv4 ACL named acl-ipv4-01:

```
switch# clear access-list counters acl-ipv4-01
switch#
```

Related Commands

Command	Description
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.

Command	Description
clear vlan access-list counters	Clears counters for VACLs.
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log [logflash]

Syntax Description

logflash	(Optional) Clears the accounting log stored in the logflash for the current VDC.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	The **logflash** keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

The **clear accounting log** command operates only in the default virtual device context (VDC 1).

This command does not require a license.

Examples

This example shows how to clear the accounting log:

```
switch# clear accounting log
```

Related Commands

Command	Description
show accounting log	Displays the accounting log contents.

clear copp statistics

To clear control plane policing (CoPP) statistics, use the **clear copp statistics** command.

clear copp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to specify a control plane class map and enter class map configuration mode:

```
switch# clear copp statistics
```

Related Commands

Command	Description
show policy-map interface control-plane	Displays the CoPP statistics for interfaces.

clear cts cache

To clear the Cisco TrustSec authentication and authorization information cache, use the **clear cts cache** command.

clear cts cache

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to clear the Cisco TrustSec authentication and authorization cache:

```
switch# clear cts cache
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

clear cts policy

To clear the Cisco TrustSec security group access control list (SGACL) policies, use the **clear cts policy** command.

clear cts policy {**all**| **peer** *device-id*| **sgt** *sgt-value*}

Syntax Description

all	Clears all the Cisco TrustSec SGACL policies on the local device.
peer *device-id*	Clears the Cisco TrustSec SGACL policies for a peer device on the local device.
sgt *sgt-value*	Clears the Cisco TrustSec SGACL policies for a security group tag (SGT) on the local device.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to clear all the Cisco TrustSec SGACL policies on the device:

```
switch# clear cts policy all
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays Cisco TrustSec SGACL policy information.

capture session

To enable a capture session for the access control list (ACL), use the capture session command.

capture session session

Syntax Description

session	Session ID. The range is from 1 to 48.

Command Default

None

Command Modes

ACL capture configuration mode (config-acl-capture)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an ACL capture session configuration:

```
switch# configure terminal
switch(config)# ip access-list abc1234
switch(config-acl)# capture session 7
switch(config-acl)#
```

Related Commands

Command	Description
ip access-list	Creates an access list.
monitor session session type acl-capture	Configures an ACL capture session.

cts dot1x

To enable Cisco TrustSec authentication on an interface and enter Cisco TrustSec 802.1X configuration mode, use the **cts dot1x** command. To revert to the default, use the **no** form of this command.

cts dot1x

no cts dot1x

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command is not supported for F1 Series modules and F2 Series modules.

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to enable Cisco TrustSec authentication on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to disable Cisco TrustSec authentication on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no cts dot1x
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts interface	Displays Cisco TrustSec configuration information for interfaces.

Related Commands

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure Layer 3 Cisco TrustSec global mapping for an SPI and subnet:

```
switch# config t
switch(config)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to remove Layer 3 global mapping for a subnet:

```
switch# config t
switch(config)# no cts l3 spi 10.10.1.1/23
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts l3 mapping	Displays the Layer 3 Cisco TrustSec mapping for SPI values to IPv4 subnets.

class (policy map)

To specify a control plane class map for a control plane policy map, use the **class** command. To delete a control plane class map from a control plane policy map, use the **no** form of this command.

class {*class-map-name* [**insert-before** *class-map-name2*]| **class-default**}

no class *class-map-name*

Syntax Description

class-map-name	Name of the class map.
insert-before *class-map-name2*	(Optional) Inserts the control plane class map ahead of another control plane class map for the control plane policy map.
class-default	Specifies the default class.

Command Default

None

Command Modes

Policy map configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to configure a class map for a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
swtich(config-pmap-c)
```

This example shows how to delete a class map from a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# no class ClassMapA
```

Related Commands

Command	Description
policy-map type control-plane	Specifies a control plane policy map and enters policy map configuration mode.
show policy-map type control-plane	Displays configuration information for control plane policy maps.

class-map type control-plane

To create or specify a control plane class map and enter class map configuration mode, use the **class-map type control-plane** command. To delete a control plane class map, use the **no** form of this command.

class-map type control-plane [**match-all| match-any**] *class-map-name*

no class-map type control-plane [**match-all| match-any**] *class-map-name*

Syntax Description

match-all	(Optional) Specifies to match all match conditions in the class map.
match-any	(Optional) Specifies to match any match conditions in the class map.
class-map-name	Name of the class map. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.

Command Default

match-any

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You cannot use match-all, match-any, or class-default as names for control plane class maps.

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to specify a control plane class map and enter class map configuration mode:

```
switch# configure terminal
switch(config)# class-map type control-plane ClassMapA
switch(config-cmap)#
```

This example shows how to delete a control plane class map:

```
switch# configure terminal
switch(config)# no class-map type control-plane ClassMapA
```

Related Commands

Command	Description
show class-map type control-plane	Displays control plane policy map configuration information.

clear aaa local user blocked

To clear the blocked local user, use the **clear local user blocked** command.

clear local user blocked username {**all**| **username**}

Syntax Description

all	Clears all the blocked users.
username	Clears the specified user.

Command Default

None

Command Modes

Any configuration mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to clear all the blocked users.

```
switch# clear aaa local user blocked all
```

Related Commands

Command	Description
aaa authentication rejected	Configures the login block per user.
show aaa authentication	Displays the AAA authentication configuration.
show aaa local user blocked	Displays the blocked local users.

clear ldap-server statistics

To clear the Lightweight Directory Access Protocol (LDAP) server statistics, use the **clear ldap-server statistics** command.

clear ldap-server statistics {**ipv4-address| ipv6-address| host-name**}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X:X* format.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

Any command mode

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 clear the statistics for an LDAP server:

```
switch# clear ldap-server statistics 10.10.1.1
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.
show ldap-server **statistics**	Displays the LDAP server statistics.

clear mac access-list counters

To clear the counters for all MAC access control lists (ACLs) or a single MAC ACL, use the **clear mac access-list counters** command.

clear mac access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the MAC ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

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 clear counters for all MAC ACLs:

```
switch# clear mac access-list counters
switch#
```

This example shows how to clear counters for a MAC ACL named acl-mac-0060:

```
switch# clear mac access-list counters acl-ipv4-0060
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear vlan access-list counters	Clears counters for VACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show mac access-lists	Displays information about one or all MAC ACLs.

clear port-security

To clear a single, dynamically learned, secure MAC address or to clear all dynamically learned, secure MAC addresses for a specific interface, use the **clear port-security** command.

clear port-security dynamic interface ethernet slot / port [**vlan vlan-id**]

clear port-security dynamic interface port-channel *channel-number* [**vlan** *vlan-id*]

clear port-security dynamic address *address* [**vlan** *vlan-id*]

Syntax Description

dynamic	Specifies that you want to clear dynamically learned, secure MAC addresses.
interface	Specifies the interface of the dynamically learned, secure MAC addresses that you want to clear.
ethernet *slot/port*	Specifies the Ethernet interface of the dynamically learned, secure MAC addresses that you want to clear.
vlan *vlan-id*	(Optional) Specifies the VLAN of the secure MAC addresses to be cleared. Valid VLAN IDs are from 1 to 4096.
port-channel *channel-number*	Specifies the port-channel interface of the dynamically learned, secure MAC addresses that you want to clear.
address *address*	Specifies a single MAC address to be cleared, where *address* is the MAC address, in dotted hexadecimal format.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Support was added for port-security on port-channel interfaces.
4.0(1)	This command was introduced.

Usage Guidelines

You must enable port security by using the **feature port-security** command before you can use the **clear port-security** command.

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# configure terminal
switch(config)# clear port-security dynamic interface ethernet 2/1
```

This example shows how to remove the dynamically learned, secure MAC address 0019.D2D0.00AE:

```
switch# configure terminal
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

Related Commands

Command	Description
debug port-security	Provides debugging information for port security.
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security	Enables port security on a Layer 2 interface.

clear cts role-based counters

To clear the role-based access control list (RBACL) statistics so that all counters are reset to 0, use the **clear cts role-based counters** command.

clear cts role-based counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command requires the Advanced Services license.

Examples

This example shows how to clear the RBACL statistics:

```
switch# clear cts role-based counters
```

Related Commands

Command	Description
cts role-based counters enable	Enables the RBACL statistics.
show cts role-based counters	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies.

clear dot1x

To clear 802.1X authenticator instances, use the **clear dot1x** command.

cleardot1x{**all**| **interface** | *slot/port*}

Syntax Description

all	Specifies all 802.1X authenticator instances.
interface ethernet *slot*/*port*	Specifies the 802.1X authenticator instances for a specified interface.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to clear all 802.1X authenticator instances:

```
switch# clear dot1x all
```

This example shows how to clear the 802.1X authenticator instances for an interface:

```
switch# clear dot1x interface ethernet 1/1
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

clear eou

To clear Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions, use the **clear eou** command.

clear eou {**all**| **authentication** {**clientless**| **eap**| **static**}| **interface ethernet slot / port**| **ip-address ipv4-address**| **mac-address mac-address**| **posturetoken type**}

Syntax Description

all	Specifies all EAPoUDP sessions.
authentication	Specifies EAPoUDP authentication.
clientless	Specifies sessions authenticated using clientless posture validation.
eap	Specifies sessions authenticated using EAPoUDP.
static	Specifies sessions authenticated using statically configured exception lists.
interface ethernet *slot*/*port*	Specifies an interface.
ip-address *ipv4-address*	Specifies an IPv4 address. in the A.B.C.D format.
mac-address *mac-address*	Specifies a MAC address.
posturetoken *type*	Specifies a posture token name.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable EAPoUDP by using the **feature eou** command before using the **clear eou** command.

This command does not require a license.

Examples

This example shows how to clear all the EAPoUDP sessions:

```
switch# clear eou all
```

This example shows how to clear the statically authenticated EAPoUDP sessions:

```
switch# clear eou authentication static
```

This example shows how to clear the EAPoUDP sessions for an interface:

```
switch# clear eou interface ethernet 1/1
```

This example shows how to clear the EAPoUDP sessions for an IP address:

```
switch# clear eou ip-address 10.10.1.1
```

This example shows how to clear the EAPoUDP sessions for a MAC address:

```
switch# clear eou mac-address 0019.076c.dac4
```

This example shows how to the EAPoUDP sessions with a posture token type of checkup:

```
switch# clear eou posturetoken healthy
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

clear hardware rate-limiter

To clear rate-limit statistics, use the **clear hardware rate-limiter** command.

clear hardware rate-limiter {**access-list-log**| **all**| **copy**| **layer-2** {**l2pt**| **mcast-snooping**| **port-security**| **storm-control**| **vpc-low**}| **layer-3** {**control**| **glean**| **glean-fast**| **mtu**| **multicast** {**directly-connected**| **local-groups**| **rpf-leak**}| **ttl**}| **receive**}

Syntax Description

access-list-log	Clears rate-limit statistics for access-list log packets.
all	Clears all rate-limit statistics.
copy	Clears rate-limit statistics for copy packets.
layer-2	Specifies Layer 2 packet rate limits.
l2pt	Clears rate-limit statistics for Layer 2 Tunnel Protocol (L2TP) packets.
mcast-snooping	Clears rate-limit statistics for Layer 2 multicast-snooping packets.
port-security	Clears rate-limit statistics for Layer 2 port-security packets.
storm-control	Clears rate-limit statistics for Layer 2 storm-control packets.
vpc-low	Clears rate-limit statistics for Layer 2 control packets over the VPC low queue.
layer-3	Specifies Layer 3 packet rate limits.
control	Clears rate-limit statistics for Layer 3 control packets.
glean	Clears rate-limit statistics for Layer 3 glean packets.
glean-fast	Clears rate-limit statistics for Layer 3 glean fast-path packets.
mtu	Clears rate-limit statistics for Layer 3 maximum transmission unit (MTU) packets.
multicast	Specifies Layer 3 multicast rate limits.
directly-connected	Clears rate-limit statistics for Layer 3 directly connected multicast packets.

local-groups	Clears rate-limit statistics for Layer 3 local group multicast packets.
rpf-leak	Clears rate-limit statistics for Layer 3 reverse path forwarding (RPF) leak multicast packets.
ttl	Clears rate-limit statistics for Layer 3 time-to-live (TTL) packets.
receive	Clears rate-limit statistics for receive packets.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	Added the glean-fast keyword.
5.0(2)	Added the **l2pt** keyword.
4.0(3)	Added the **port-security** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

You can use the command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to clear all the rate-limit statistics:

```
switch# clear hardware rate-limiter all
```

This example shows how to clear the rate-limit statistics for access-list log packets:

```
switch# clear hardware rate-limiter access-list-log
```

This example shows how to clear the rate-limit statistics for Layer 2 storm-control packets:

```
switch# clear hardware rate-limiter layer-2 storm-control
```

This example shows how to clear the rate-limit statistics for Layer 3 glean packets:

```
switch# clear hardware rate-limiter layer-3 glean
```

This example shows how to clear the rate-limit statistics for Layer 3 directly connected multicast packets:

```
switch# clear hardware rate-limiter layer-3 multicast directly-connected
```

This example shows how to clear the rate-limit statistics for received packets:

```
switch# clear hardware rate-limiter receive
```

Related Commands

Command	Description
hardware rate-limiter	Configures rate limits.
show hardware rate-limiter	Displays rate-limit information.

clear ip arp inspection log

To clear the Dynamic ARP Inspection (DAI) logging buffer, use the **clear ip arp inspection log** command.

clear ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 clear the DAI logging buffer:

```
switch# clear ip arp inspection log
switch#
```

Related Commands

Command	Description
ip arp inspection log-buffer	Configures the DAI logging buffer size.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection statistics	Displays the DAI statistics.

clear ip access-list counters

To clear the counters for all IPv4 access control lists (ACLs) or a single IPv4 ACL, use the **clear ip access-list counters** command.

clear ip access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv4 ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

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 clear counters for all IPv4 ACLs:

```
switch# clear ip access-list counters
switch#
```

This example shows how to clear counters for an IP ACL named acl-ipv4-101:

```
switch# clear ip access-list counters acl-ipv4-101
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.
clear vlan access-list counters	Clears counters for VACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show ip access-lists	Displays information about one or all IPv4 ACLs.

clear ip arp inspection statistics vlan

To clear the Dynamic ARP Inspection (DAI) statistics for a specified VLAN, use the **clear ip arp inspection statistics vlan** command.

clear ip arp inspection statistics vlan *vlan-list*

Syntax Description

vlan *vlan-list*	Specifies the VLANs whose DAI statistics this command clears. 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 4094.

Command Default

None

Command Modes

Any command mode

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 clear the DAI statistics for VLAN 2:

```
switch# clear ip arp inspection statistics vlan 2
switch#
```

This example shows how to clear the DAI statistics for VLANs 5 through 12:

```
switch# clear ip arp inspection statistics vlan 5-12
switch#
```

This example shows how to clear the DAI statistics for VLAN 2 and VLANs 5 through 12:

```
switch# clear ip arp inspection statistics vlan 2,5-12
switch#
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.

Command	Description
ip arp inspection log-buffer	Configures the DAI logging buffer size.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection vlan	Displays DAI status for a specified list of VLANs.

clear ip device tracking

To clear IP device tracking information, use the **clear ip device tracking** command.

clear ip device tracking {**all**| **interface ethernet slot** / **port**| **ip-address ipv4-address**| **mac-address mac-address**}

Syntax Description

all	Clears all IP device tracking information.
interface ethernet *slot*/*port*	Clears IP device tracking information for an interface.
ip-address *ipv4-address*	Clears IP device tracking information for an IPv4 address in the A.B.C.D format.
mac-address *mac-address*	Clears IP tracking information for a MAC address in the XXXX.XXXX.XXXX format.

Command Default

None

Command Modes

Any command mode

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 clear all the IP device tracking information:

```
switch# clear ip device tracking all
```

This example shows how to clear the IP device tracking information for an interface:

```
switch# clear ip device tracking interface ethernet 1/1
```

This example shows how to clear the IP device tracking information for an IP address:

```
switch# clear ip device tracking ip-address 10.10.1.1
```

This example shows how to clear the IP device tracking information for a MAC address:

```
switch# clear ip device tracking mac-address 000c.30da.86f4
```

Related Commands

Command	Description
ip device tracking	Enables IP device tracking.
show ip device tracking	Displays IP device tracking information.

clear ip dhcp relay statistics

To clear the DHCP relay statistics, use the **clear ip dhcp relay statistics** command.

clear ip dhcp relay statistics [**interface interface**]

Syntax Description

interface *interface*	(Optional) Clears the DHCP relay statistics for a specific interface. The supported interface types are ethernet, port-channel, and VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the global DHCP relay statistics:

```
switch# clear ip dhcp relay statistics
```

Related Commands

Command	Description
ip dhcp relay	Enables the DHCP relay agent.
show ip dhcp relay statistics	Displays the DHCP relay statistics.

clear ip dhcp snooping binding

To clear the DHCP snooping binding database, use the **clear ip dhcp snooping binding** command.

clear ip dhcp snooping binding

clear ip dhcp snooping binding [**vlan vlan-id mac mac-address ip ip-address interface ethernet slot** / **port** [. **subinterface-number**]]

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface port-channel** *channel-number* [. *subchannel-number*]]

Syntax Description

vlan *vlan-id*	(Optional) Clears the DHCP snooping binding database for an entry identified with the VLAN ID specified by the *vlan-id* argument and the additional keywords and arguments that follow.
mac-address *mac-address*	Specifies the MAC address of the binding database entry to be cleared. Enter the *mac-address* argument in dotted hexadecimal format.
ip *ip-address*	Specifies the IPv4 address of the binding database entry to be cleared. Enter the *ip-address* argument in dotted decimal format.
interface ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface of the binding database entry to be cleared.
.*subinterface-number*	(Optional) Number of the Ethernet-interface subinterface. **Note** The dot separator is required between the *port* and *subinterface-number* arguments.
interface port-channel *channel-number*	(Optional) Specifies the Ethernet port-channel of the binding database entry to be cleared.
.*subchannel-number*	(Optional) Number of the Ethernet port-channel subchannel. **Note** The dot separator is required between the *channel-number* and *subchannel-number* arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(3)	This command was modified to support clearing a specific binding database entry. The optional **vlan** keyword and the arguments and keywords that follow it were added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the DHCP snooping binding database:

```
switch# clear ip dhcp snooping binding
switch#
```

This example shows how to clear a specific entry from the DHCP snooping binding database:

```
switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface
ethernet 2/11
switch#
```

Related Commands

Command	Description
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping	Displays general information about DHCP snooping.
show ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.
show ip dhcp snooping statistics	Displays DHCP snooping statistics.
show running-config dhcp	Displays DHCP snooping configuration, including the IP Source Guard configuration.

clear ipv6 access-list counters

To clear the counters for all IPv6 access control lists (ACLs) or a single IPv6 ACL, use the **clear ipv6 access-list counters** command.

clear ipv6 access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the IPv6 ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

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 clear counters for all IPv6 ACLs:

```
switch# clear ipv6 access-list counters
switch#
```

This example shows how to clear counters for an IPv6 ACL named acl-ipv6-3A:

```
switch# clear ipv6 access-list counters acl-ipv6-3A
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.
clear vlan access-list counters	Clears counters for VACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show ipv6 access-lists	Displays information about one or all IPv6 ACLs.

clear ipv6 dhcp relay statistics

To clear the DHCPv6 relay statistics, use the **clear ipv6 dhcp relay statistics** command.

clear ipv6 dhcp relay statistics [**interface interface**]

Syntax Description

interface *interface*	(Optional) Clears the DHCPv6 relay statistics for a specific interface. The supported interface types are ethernet, port-channel, and VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the global DHCPv6 relay statistics:

```
switch# clear ipv6 dhcp relay statistics
```

Related Commands

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

clear ipv6 dhcp-ldra statistics

To clear Lightweight DHCPv6 Relay Agent (LDRA) related statistics, use the clear ipv6 dhcp-ldra statistics command.

clear ipv6 dhcp-ldra statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

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 and LDRA feature.

Examples

This example shows how to clear the LDRA related statistics:

```
switch# clear ipv6 dhcp-ldra statistics
```

Related Commands

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

clear vlan access-list counters

To clear the counters for all VLAN access control lists (VACLs) or a single VACL, use the **clear vlan access-list counters** command.

clear vlan access-list counters [*access-map-name*]

Syntax Description

access-map-name	(Optional) Name of the VLAN access map whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Privileged EXEC

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 clear counters for all VACLs:

```
switch# clear vlan access-list counters
switch#
```

This example shows how to clear counters for a VACL named vlan-map-101:

```
switch# clear vlan access-list counters vlan-map-101
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear mac access-list counters	Clears counters for MAC ACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show vlan access-map	Displays information about one or all VACLs.

conf-offset

To configure the confidentiality offset for MACsec Key Agreement (MKA) encryption, use the **conf-offset** command. To disable the confidentiality offset, use the **no** form of this command.

conf-offset {**CONF-OFFSET-0** | **CONF-OFFSET-30** | **CONF-OFFSET-50**}

no conf-offset {**CONF-OFFSET-0** | **CONF-OFFSET-30** | **CONF-OFFSET-50**}

Syntax Description

CONF-OFFSET-0	Does not offset the encryption.
CONF-OFFSET-30	Offsets the encryption by 30 characters.
CONF-OFFSET-50	Offsets the encryption by 50 characters.

Command Default

No confidentiality offset is configured for MKA encryption.

Command Modes

MACsec policy configuration (config-macsec-policy)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, you should enable the MKA feature first.

Examples

This example shows how to set the confidentiality offset:

```
switch# configure terminal
switch(config)# macsec policy p1
switch(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.

Command	Description
macsec keychain policy	Configures a MACsec keychain policy.
macsec policy	Configures a MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACSec policies in the system.
show run mka	Displays the status of MKA.

copp copy profile

To create a copy of the Control Plane Policing (CoPP) best practice policy, use the copp clone profile command.

copp copy profile {**lenient**| **moderate**| **strict**} {**prefix**| **suffix**} **string**

Syntax Description

lenient	Specifies the lenient profile.
moderate	Specifies the moderate profile.
strict	Specifies the strict profile.
prefix	Specifies a prefix for the cloned policy.
suffix	Specifies a suffix for the cloned policy.
string	Prefix or suffix string. The suffix or prefix can be any alphanumeric string up to 20 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

When you use the copp copy profile command, CoPP renames all class maps and policy maps with the specified prefix or suffix.

This command does not require a license.

Examples

This example shows how to create a clone of the CoPP best practice policy:

```
switch # copp copy profile moderate abc
```

Related Commands

Command	Description
copp profile	Applies the default CoPP best practice policy on the Cisco NX-OS device.
show copp status	Displays the CoPP status, including the last configuration operation and its status.
show running-config copp	Displays the CoPP configuration in the running configuration.

copp profile

To apply the default Control Plane Policing (CoPP) best practice policy on the Cisco NX-OS device without rerunning the setup utility, use the copp profile command. To remove the default CoPP policy from the Cisco NX-OS device, use the no form of this command.

copp profile {**dense**| **lenient**| **moderate**| **strict**}

no copp profile {**dense**| **lenient**| **moderate**| **strict**}

Syntax Description

dense	Specifies the dense profile.
lenient	Specifies the lenient profile.
moderate	Specifies the moderate profile.
strict	Specifies the strict profile.

Command Default

strict

Command Modes

Global configuration (config)

Command History

Release	Modification
5.2(1)	This command was introduced.
6.0(1)	Added the dense keyword.

Usage Guidelines

In Cisco NX-OS releases prior to 5.2(1), you must use the setup utility to change or reapply the default CoPP policy. You can access the setup utility using the setup command.

Beginning with Cisco NX-OS Release 5.2, the CoPP best practice policy is read-only. If you want to modify its configuration, you must clone it using the copp clone profile command. Cloned policies are treated as user configurations.

When you use in-service software downgrade (ISSU) to upgrade to Cisco NX-OS Release 5.2, the policy attached to the control plane is treated as a user-configured policy. Check the CoPP profile using the show copp profile command and make any required changes.

If you use ISSU to downgrade from Cisco NX-OS Release 5.2, CoPP reports the incompatible configuration and instructs you to clone the CoPP profile. In the lower version, all configurations are restored in user-configuration mode.

This command does not require a license.

Examples

This example shows how to apply the default CoPP best practice policy on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# copp profile moderate
switch(config)#
```

This example shows how remove the default CoPP best practice policy from the Cisco NX-OS device:

```
switch(config)# no copp profile moderate
switch(config)#
```

Related Commands

Command	Description
copp copy profile	Creates a copy of the CoPP best practice policy.
show copp profile	Displays the details of the CoPP best practice policy.
show copp status	Displays the CoPP status, including the last configuration operation and its status.
show running-config copp	Displays the CoPP configuration in the running configuration.

CRLLookup

To configure the attribute name, search filter, and base-DN for the certificate revocation list (CRL) search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **CRLLookup** command. To disable this configuration, use the **no** form of this command.

CRLLookup attribute-name attribute-name search-filter filter base-DN *base-DN-name*

no CRLLookup

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base-designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

Lightweight Directory Access Protocol (LDAP) search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the CRL search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# CRLLookup attribute-name certificateRevocationList
search-filter (&(objectClass=cRLDistributionPoint)) base-DN CN=CDP,CN=Public Key
Services,CN=Services,CN=Configuration,DC=mdsldaptestlab,DC=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

crypto ca authenticate

To associate and authenticate a certificate of the certificate authority (CA) and configure its CA certificate (or certificate chain), use the **crypto ca authenticate** command. To remove the association and authentication, use the **no** form of this command.

crypto ca authenticate *trustpoint-label*

no crypto ca authenticate *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The name The name is alphanumeric, case sensitive, and has a maximum length of 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You can use this command to authenticate the CA to the Cisco NX-OS device by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you execute this command. The CA certificate or certificate chain must be available in Privacy Enhanced Mail (PEM) (base-64) encoded format.

Use this command when you initially configure certificate authority support for the device. First create the trustpoint using the **crypto ca trustpoint** command using the CA certificate fingerprint published by the CA. You must compare the certificate fingerprint displayed during authentication with the one published by the CA and accept the CA certificate only if it matches.

If the CA to authenticate is a subordinate CA (it is not self-signed), then another CA certifies it, which in turn may be certified by yet another CA, and so on, until there is a self-signed CA. In this case, the subordinate CA has a CA certificate chain. You must enter the entire chain during CA authentication. The maximum length that the CA certificate chain supports is ten.

The trustpoint CA is the certificate authority that you configure on the device as the trusted CA. The device accepts any peer certificate if it is signed by a locally trusted CA or its subordinates.

The trustpoint configuration that you create with the **crypto ca trustpoint** command persists across device reboots only if you save it explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trustpoint are automatically persistent when you save the trustpoint configuration in the startup configuration. Otherwise, if you do not saved the trustpoint in the startup configuration, the associated certificates and CRL are not automatically persistent because they cannot exist without the corresponding trustpoint after the device reboots.

To ensure that the configured certificates, CRLs, and key pairs are persistent, always save the running configuration in the startup configuration.

This command does not require a license.

Examples

This example shows how to authenticate a CA certificate called admin-ca:

```
switch# configure terminal
switch(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
 END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]: y
```

Related Commands

Command	Description
crypto ca trustpoint	Configures the trustpoint.
show crypto ca certificates	Displays configured trustpoint certificates.
show crypto ca trustpoints	Displays trustpoint configurations.

crypto ca crl request

To configure a new certificate revocation list (CRL) downloaded from the certificate authority (CA), use the **crypto ca crl request** command.

crypto ca crl request *trustpoint-label source-file*

Syntax Description

trustpoint-label	Name of the trustpoint. The maximum size is 64 characters.
source-file	Location of the CRL in the form **bootflash**:*filename* . The maximum size is 512.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

The crypto ca crl request command allows you to pre-download CRLs for the trustpoints and cache the CRLs in the certificate (cert) store. The CRL file specified should contain the latest CRL in either the Privacy Enhanced Mail (PEM) format or Distinguished Encoding Rules (DER) format.

The trustpoint configuration that you create with the **crypto ca trustpoint** command persists across device reboots only if you save it explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trustpoint are automatically persistent when you save the trustpoint configuration in the startup configuration. Otherwise, if you do not save the trustpoint in the startup configuration, the associated certificates and CRL are not automatically persistent because they cannot exist without the corresponding trustpoint after the device reboots.

To ensure that the configured certificates, CRLs and key pairs are persistent, always save the running configuration in the startup configuration.

This command does not require a license.

Examples

This example shows how to configure a CRL for the trustpoint or replaces the current CRL:

```
switch# configure teminal
switch(config)# crypto ca crl request admin-ca bootflash:admin-ca.crl
```

Related Commands

Command	Description
revocation-check	Configures trustpoint revocation check methods.
show crypto ca crl	Displays configured certificate revocation lists (CRL).

clear ldap-server statistics

To clear the Lightweight Directory Access Protocol (LDAP) server statistics, use the **clear ldap-server statistics** command.

clear ldap-server statistics {**ipv4-address| ipv6-address| host-name**}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X:X* format.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

Any command mode

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 clear the statistics for an LDAP server:

```
switch# clear ldap-server statistics 10.10.1.1
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.
show ldap-server **statistics**	Displays the LDAP server statistics.

clear mac access-list counters

To clear the counters for all MAC access control lists (ACLs) or a single MAC ACL, use the **clear mac access-list counters** command.

clear mac access-list counters [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of the MAC ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

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 clear counters for all MAC ACLs:

```
switch# clear mac access-list counters
switch#
```

This example shows how to clear counters for a MAC ACL named acl-mac-0060:

```
switch# clear mac access-list counters acl-ipv4-0060
switch#
```

Related Commands

Command	Description
clear access-list counters	Clears counters for IPv4, IPv6, and MAC ACLs.
clear ip access-list counters	Clears counters for IPv4 ACLs.
clear ipv6 access-list counters	Clears counters for IPv6 ACLs.
clear vlan access-list counters	Clears counters for VACLs.

Command	Description
show access-lists	Displays information about one or all IPv4, IPv6, and MAC ACLs.
show mac access-lists	Displays information about one or all MAC ACLs.

clear port-security

To clear a single, dynamically learned, secure MAC address or to clear all dynamically learned, secure MAC addresses for a specific interface, use the **clear port-security** command.

clear port-security dynamic interface ethernet slot / port [**vlan vlan-id**]

clear port-security dynamic interface port-channel *channel-number* [**vlan** *vlan-id*]

clear port-security dynamic address *address* [**vlan** *vlan-id*]

Syntax Description

dynamic	Specifies that you want to clear dynamically learned, secure MAC addresses.
interface	Specifies the interface of the dynamically learned, secure MAC addresses that you want to clear.
ethernet *slot/port*	Specifies the Ethernet interface of the dynamically learned, secure MAC addresses that you want to clear.
vlan *vlan-id*	(Optional) Specifies the VLAN of the secure MAC addresses to be cleared. Valid VLAN IDs are from 1 to 4096.
port-channel *channel-number*	Specifies the port-channel interface of the dynamically learned, secure MAC addresses that you want to clear.
address *address*	Specifies a single MAC address to be cleared, where *address* is the MAC address, in dotted hexadecimal format.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Support was added for port-security on port-channel interfaces.
4.0(1)	This command was introduced.

Usage Guidelines

You must enable port security by using the **feature port-security** command before you can use the **clear port-security** command.

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# configure terminal
switch(config)# clear port-security dynamic interface ethernet 2/1
```

This example shows how to remove the dynamically learned, secure MAC address 0019.D2D0.00AE:

```
switch# configure terminal
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

Related Commands

Command	Description
debug port-security	Provides debugging information for port security.
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security	Enables port security on a Layer 2 interface.

clear radius-server statistics

To clear the statistics for a RADIUS server host, use the **clear radius-server statistics** command.

clear radius-server statistics {*ipv4-address*| *ipv6-address*| *server-name*}

Syntax Description

ipv4-address	IPv4 address of a RADIUS server host in *A.B.C.D* format.
ipv6-address	IPv6 address of a RADIUS server host in *A:B::C:D* format.
server-name	Name of a RADIUS server host. The name is case sensitive.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear statistics for a RADIUS server:

```
switch# clear radius-server statistics 10.10.1.1
```

Related Commands

Command	Description
show radius-server statistics	Displays RADIUS server host statistics.

clear ssh hosts

To clear the Secure Shell (SSH) host sessions and the known host file for a virtual device context (VDC), use the **clear ssh hosts** command.

clear ssh hosts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 clear all SSH host sessions and the known host file:

```
switch# clear ssh hosts
```

Related Commands

Command	Description
ssh server enable	Enables the SSH server.

clear tacacs-server statistics

To clear the statistics for a TACACS+ server host, use the **clear tacacs-server statistics** command.

clear tacacs-server statistics {*ipv4-address*| *ipv6-address*| *server-name*}

Syntax Description

ipv4-address	IPv4 address of a TACACS+ server host in *A.B.C.D* format.
ipv6-address	IPv6 address of a TACACS+ server host in *A:B::C:D* format.
server-name	Name of a TACACS+ server host. The name is case sensitive.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear statistics for a TACACS+ server:

```
switch# clear tacacs-server statistics 10.10.1.1
```

Related Commands

Command	Description
show tacacs-server statistics	Displays TACACS+ server host statistics.

clear user

To clear a user session for a virtual device context (VDC), use the **clear user** command.

clear user *user-id*

Syntax Description

user-id	User identifier.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **show users** command to display the current user sessions on the device.

This command does not require a license.

Examples

This example shows how to clear all SSH host sessions:

```
switch# clear user user1
```

Related Commands

Command	Description
show users	Displays the user session information.

cts l3 spi (global)

To enable Layer 3 Cisco TrustSec and map a security parameter index (SPI) and subnet for the device, use the **cts l3 spi** command. To remove the mapping to an IPv4 subnet, use the **no** form of this command.

ctsl3 **spi A.B.C.D** / *length*

no ctsl3 **spi A.B.C.D** / *length*

Syntax Description

spi-number	SPI for the device. The range is from 0 to 429496729.
A.B.C.D/length	IPv4 subnet.

Command Default

None

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 Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure Layer 3 Cisco TrustSec global mapping for an SPI and subnet:

```
switch# config t
switch(config)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to remove Layer 3 global mapping for a subnet:

```
switch# config t
switch(config)# no cts l3 spi 10.10.1.1/23
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 mapping	Displays the Layer 3 Cisco TrustSec mapping for SPI values to IPv4 subnets.

cts l3 spi (interface)

To enable Layer 3 Cisco TrustSec and configure a security parameter index (SPI) on an interface, use the **cts l3 spi** command. To revert to the default, use the **no** form of this command.

cts l3 spi *spi-number*

no cts l3

Syntax Description

spi-number	SPI for the interface. The range is from 0 to 429496729.

Command Default

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 Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to disable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts l3
```

Related Commands

Command	Description
cts l3 spi (global)	Enables the Layer 3 Cisco TrustSec for the device.
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 interface	Displays the Layer 3 Cisco TrustSec configuration on the interfaces.

crypto ca enroll

To request a certificate for the device RSA key pair created for this trustpoint CA, use the **crypto ca enroll** command.

crypto ca enroll *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The maximum size is 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

A Cisco NX-OS device enrolls with the trustpoint CA to obtain an identity certificate. You can enroll your device with multiple trustpoints and obtain a separate identity certificate from each trustpoint.

When enrolling with a trustpoint, you must specify an RSA key pair to certify. You must generate the key pair and associate it to the trustpoint before generating the enrollment request.

Use the crypto ca enroll command to generate a request to obtain an identity certificate from each of your trustpoints that correspond to authenticated CAs. The certificate signing request (CSR) generated is per the Public-Key Cryptography Standards (PKCS) #10 standard and is displayed in the PEM format. You then cut and paste the certificate and submit it to the corresponding CA through an e-mail or on the CA website. The CA administrator issues the certificate and makes it available to you either through the website or by sending it in an e-mail. You need to import the obtained identity certificate that corresponds to the trustpoint using the **crypto ca import** *trustpoint-label* **certificate** command.

Note The device does not save the challenge password with the configuration. Record this password so that you can provide it if you need to revoke your certificate.

This command does not require a license.

Examples

This example shows how to generate a certificate request for an authenticated CA:

```
switch# configure terminal
switch(config)# crypto ca enroll myCA
```

```
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:nbv123
 The subject name in the certificate will be: Vegas-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]:no
 Include an IP address in the subject name [yes/no]:yes
ip address:209.165.200.226
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

Related Commands

Command	Description
crypto ca import trustpoint-label certificate	Imports the identity certificate obtained from the CA to the trustpoint.
crypto key generate rsa	Generates an RSA key pair.
rsakeypair	Configures and associates the RSA key pair details to a trustpoint.
show crypto key mypubkey rsa	Displays all RSA public key configurations.

crypto ca export

To export the RSA key pair and the associated certificates (identity and CA) of a trustpoint within a Public-Key Cryptography Standards (PKCS) #12 format file to a specified location, use the **crypto ca export** command.

crypto ca export *trustpoint-label* **pkcs12** *destination-file-url pkcs12-password*

Syntax Description

trustpoint-label	Name of the trustpoint. The maximum size is 64 characters.
pkcs12 *destination-file-url*	Specifies a destination file in **bootflash**:*filename* format. The filename is alphanumeric, case sensitive, and has maximum of 512 characters.
*pkcs 12***-***password*	Password to be used to protect the RSA private key in the exported file. The passwords is alphanumeric, case sensitive, and has maximum of 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You can export the identity certificate with the associated RSA key pair and CA certificate (or certificate chain) to a PKCS #12 format file for backup purposes. You can later import the certificate and RSA key pair to recover from a system crash on your device.

This command does not require a license.

Examples

This example shows how to export a certificate and key pair in the PKCS #12 format:

```
switch# configure terminal
switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

Related Commands

Command	Description
crypto ca import trustpoint-label certificate	Imports the identity certificate obtained from the CA to the trustpoint.
crypto ca import trustpoint-label pkcs12	Imports the identity certificate and associated RSA key pair and CA certificate (chain) to a trustpoint.
crypto key generate rsa	Generates an RSA key pair.
rsakeypair	Configures and associates the RSA key pair details to a trustpoint.
show crypto key mypubkey rsa	Displays any RSA public key configurations.

crypto ca import

To import the identity certificate in the Privacy Enhanced Mail (PEM) format or the identity certificate and associated RSA key pair and CA certificate (or certificate chain) in the Public-Key Cryptography Standards (PKCS) #12 format, use the **crypto ca import** command.

crypto ca import *trustpoint-label* {**certificate**| **pkcs12** *source-file-url pkcs12- password* }

Syntax Description

trustpoint-label	Name of the trustpoint. The maximum size is 64 characters.
certificate	Specifies that you will paste the trustpoint certificate at the command-line interface (CLI) prompt.
pkcs12 *source-file-url pkcs12-*	Specifies a source file containing the trustpoint certificate in **bootflash**:*filename* format. The filename is case sensitive.
password	Password that was used to protect the RSA private key in the imported PKCS#12 file. The password is case sensitive.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **certificate** keyword to import (by cut and paste means) the identity certificate obtained from the CA, corresponding to the enrollment request generated earlier in the trustpoint and submitted to the CA.

Use the **pkcs12** *source-file-url pkcs12-password* keyword and argumen t to import the complete identity information, which includes the identity certificate and associated RSA key pair and CA certificate or certificate chain, into an empty trustpoint. This method allows you to restore the configuration after a system crash.

The trustpoint configuration that you create with the **crypto ca trustpoint** command persists across device reboots only if you save it explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trustpoint are automatically persistent when you save the trustpoint configuration in the startup configuration. Otherwise, if you do not saved the trustpoint in the startup configuration, the associated certificates and CRL are not automatically persistent because they cannot exist without the corresponding trustpoint after the device reboots.

To ensure that the configured certificates, CRLs and key pairs are persistent, always save the running configuration in the startup configuration.

This command does not require a license.

Examples

This example shows how to install an identity certificate obtained from a CA corresponding to an enrollment request made and submitted earlier:

```
switch# configure terminal
switch(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

This example shows how to import a certificate and key pair in a Public-Key Cryptography Standards (PKCS) #12 format file:

```
switch# configure terminal
witch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

Related Commands

Command	Description
crypto ca export trustpoint-label pkcs12	Exports the RSA key pair and associated certificates of a trustpoint.
crypto ca enroll	Generates a certificate signing request for a trustpoint.
crypto key generate rsa	Generates the RSA key pair.
rsakeypair	Configures trustpoint RSA key pair details.
show crypto ca certificates	Displays the identity and CA certificate details.
show crypto key mypubkey rsa	Displays any RSA public key configurations.

crypto ca lookup

To specify the cert-store to be used for certificate authentication, use the **crypto ca lookup** command.

crypto ca lookup {**local**| **remote**| **both**}

Syntax Description

local	Specifies the local cert-store for certificate authentication.
remote	Specifies the remote cert-store for certificate authentication.
both	Specifies the local cert-store for certificate authentication, but if the authentication fails or the CA certificate is not found, the remote cert-store is used.

Command Default

Local

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

If you plan to configure a remote cert-store, you must set up an LDAP server in a remote device and make sure that the CA certificates that are used for authentication are loaded to the Active Directory.

This command does not require a license.

Examples

This example shows how to specify the remote cert-store for certificate authentication:

```
switch(config)# crypto ca lookup remote
```

Related Commands

Command	Description
crypto ca remote ldap crl-refresh-time	Configures the refresh time to update the certificate revocation list from the remote cert-store.

Command	Description
crypto ca remote ldap server-group	Configures the LDAP server group to be used while communicating with LDAP.
show crypto ca certstore	Displays the configured cert-store.
show crypto ca remote-certstore	Displays the remote cert-store configuration.

crypto ca remote ldap crl-refresh-time

To configure the refresh time to update the certificate revocation list (CRL) from the remote cert-store, use the **crypto ca remote ldap crl-refresh-time** command.

crypto ca remote ldap crl-refresh-time hours

Syntax Description

hours	Refresh time value in hours. The range is from 0 to 744 hours. If you enter 0, the refresh routine runs once.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must configure a remote cert-store and the LDAP server group.

This command does not require a license.

Examples

This example shows how to configure the refresh time to update the CRL from the remote cert-store:

```
switch(config)# crypto ca remote ldap crl-refresh-time 10
```

Related Commands

Command	Description
crypto ca lookup	Specifies the cert-store to be used for certificate authentication.
crypto ca remote ldap server-group	Configures the LDAP server group to be used while communicating with LDAP.

crypto ca remote ldap server-group

To configure the Lightweight Directory Access Protocol (LDAP) server group to be used while communicating with LDAP, use the **crypto ca remote ldap server-group** command.

crypto ca remote ldap server-group group-name

Syntax Description

group-name	Server group name. You can enter up to 64 alphanumeric characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must configure a remote cert-store.

This command does not require a license.

Examples

This example shows how to configure the LDAP server group to be used while communicating with LDAP:

```
switch(config)# crypto ca remote ldap server-group group1
```

Related Commands

Command	Description
crypto ca lookup	Specifies the cert-store to be used for certificate authentication.
crypto ca remote ldap crl-refresh-time	Configures the refresh time to update the certificate revocation list from the remote cert-store.

crypto ca test verify

To verify a certificate file, use the **crypto ca test verify** command.

crypto ca test verify *certificate-file*

Syntax Description

certificate-file	Certificate filename in the form **bootflash**:*filename* . The filename is case sensitive.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use this command to verify the specified certificate in the PEM format by using the trusted CAs configured and by consulting the certificate revocation list (CRL), if needed, as indicated by the revocation checking configuration.

This command does not require a license.

Examples

This example shows how to verify a certificate file:

```
switch(config)# crypto ca test verify bootflash:id1.pem
verify status oode:0
verify error msg:
```

Note The verify status code value of 0 indicates that the verification is successful.

Related Commands

Command	Description
show crypto ca certificates	Displays configured trustpoint certificates.

crypto ca trustpoint

To create a trustpoint certificate authority (CA) that the device should trust and enter trustpoint configuration mode, use the **crypto ca trustpoint** command. To remove the trustpoint, use the **no** form of this command.

crypto ca trustpoint *trustpoint-label*

no crypto ca trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Trustpoints have the following characteristics:

- A trustpoint corresponds to a single CA, which a Cisco NX-OS device trusts for peer certificate verification for any application.
- A CA must be explicitly associated to a trustpoint using the **crypto ca authenticate** command.
- A Cisco NX-OS device can have many trustpoints and all applications on the device can trust a peer certificate issued by any of the trustpoint CAs.
- A trustpoint is not restricted to a specific application.
- The Cisco NX-OS device can optionally enroll with a trustpoint CA to get an indemnity certificate for itself.

You do not need to designate one or more trustpoints to an application. Any application should be able to use any certificate issued by any trustpoint as long as the certificate satisfies the application requirement.

You do not need more than one identity certificate from a trustpoint or more than one key pair associated to a trustpoint. A CA certifies a given identity (name) only once and does not issue multiple certificates with the same subject name. If you need more than one identity certificate for a CA, define another trustpoint for the same CA, associate another key pair to it, and have it certified if the CA allows multiple certificates with the same subject name.

Note Before using the **no crypto ca trustpoint** command to remove the trustpoint, you must first delete the identity certificate and CA certificate (or certificate chain) and then disassociate the RSA key pair from the trustpoint. The device enforces this sequence of actions to prevent the accidental removal of the trustpoint with the certificates.

This command does not require a license.

Examples

This example shows how to declare a trustpoint CA that the device should trust and enter trustpoint configuration mode:

```
switch#
configure terminal

switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)#
```

This example shows how to remove the trustpoint CA:

```
switch#
configure terminal

switch(config)# no crypto ca trustpoint admin-ca
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the certificate authority.
crypto ca enroll	Generates a certificate signing request for a trustpoint.
show crypto ca certificates	Displays the identity and CA certificate details.
show crypto ca trustpoints	Displays trustpoint configurations.

crypto cert ssh-authorize

To configure a certificate mapping filter for the SSH protocol, use the **crypto cert ssh-authorize** command.

crypto cert ssh-authorize [**default**| **issuer-CAname**] [**map map-name1 [map-name2]**]

Syntax Description

default	Specifies the default filter map for SSH authorization.
issuer-CAname	Issuer of the CA certificate. You can enter up to 64 alphanumeric characters. You can enter up to 64 alphanumeric characters.
map	Specifies the mapping filter to be applied.
map-name1, map-name2	Name of the default mapping filter, which is already configured. You can enter up to 64 alphanumeric characters. If you do not use the default map, you can specify one or two filter maps for authorization.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must create a filter map.

This command does not require a license.

Examples

This example shows how to configure a certificate mapping filter for the SSH protocol:

```
switch(config)# crypto cert ssh-authorize default map
 filtermap1
```

Related Commands

Command	Description
crypto certificatemap mapname	Creates a filter map.
filter	Configures one or more certificate mapping filters within the filter map.
show crypto ssh-auth-map	Displays the mapping filters configured for SSH authentication.

crypto certificatemap mapname

To create a filter map, use the **crypto certificatemap mapname** command.

crypto certificatemap mapname *map-name*

Syntax Description

map-name	Name of the filter map. You can enter up to 64 alphanumeric characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must configure a cert-store for certificate authentication.

This command does not require a license.

Examples

This example shows how to create a new filter map:

```
switch(config)# crypto certificatemap mapname
 filtermap1
```

Related Commands

Command	Description
filter	Configures one or more certificate mapping filters within the filter map.
show crypto certificatemap	Displays the certificate mapping filters.

cts cache enable

To enable Cisco TrustSec authentication and authorization information caching, use the **cts cache enable** command. To revert to the default, use the **no** form of this command.

cts cache enable

no cts cache enable

Syntax Description

This command has no arguments or keywords.

Command Default

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 Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Cisco TrustSec authentication and authorization caching:

```
switch# config t
switch(config)# cts cache enable
```

This example shows how to disable Cisco TrustSec authentication and authorization caching:

```
switch# config t
switch(config)# no cts cache enable
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts	Displays Cisco TrustSec configuration information.

cts device-id

To configure a Cisco TrustSec device identifier, use the **cts device-id** command.

cts device-id *device-id* **password [7]** *password*

Syntax Description

device-id	Cisco TrustSec device identifier name. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.
7	(Optional) Encrypts the password.
password *password*	Specifies the password to use during EAP-FAST processing. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.

Command Default

No Cisco TrustSec device identifier

Clear text password

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 Cisco TrustSec feature using the **feature cts** command.

The Cisco TrustSec device identifier name must be unique in your Cisco TrustSec network cloud.

This command requires the Advanced Services license.

Examples

This example shows how to configure a Cisco TrustSec device identifier:

```
switch# configure terminal
swtich(config)# cts device-id DeviceA password Cisco321
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts credentials	Displays the Cisco TrustSec credentials information.

cts role-based sgt-map

To manually configure the Cisco TrustSec security group tag (SGT) mapping to IP addresses, use the **cts role-based sgt-map** command. To remove an SGT, use the **no** form of this command.

cts role-based sgt-map *ipv4-address sgt-value*

no cts role-based sgt-map *ipv4-address*

Syntax Description

ipv4-address	IPv4 address. The format is *A.B.C.D*
sgt-value	SGT value. The range is 0 to 65533.

Command Default

None

Command Modes

Global configuration VLAN configuration VRF configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure mapping for a Cisco TrustSec SGT:

```
switch# configure terminal
switch(config)# cts role-based sgt-map 10.10.1.1 3
switch(config-rbacl)#
```

This example shows how to remove a Cisco TrustSec SGT mapping:

```
switch# configure terminal
switch(config)# no ccts role-based sgt-map 10.10.1.1
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based sgt-map	Displays the Cisco TrustSec SGT mapping.

cts sgt

To configure the security group tag (SGT) for Cisco TrustSec, use the **cts sgt** command.

cts sgt *tag*

Syntax Description

tag	Local SGT for the device that is a decimal value or a hexadecimal value with the format **0x***hhhh* . The decimal range is from 2 to 65519, and the hexadecimal range is from 0x0 to 0xffff.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
6.2(2)	Modified the tag argument to accept decimal values.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to configure the Cisco TrustSec SGT for the device:

```
switch# configure terminal
switch(config)# cts sgt 0x3
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts environment-data	Displays the Cisco TrustSec environment data.

cts l3 spi (global)

To enable Layer 3 Cisco TrustSec and map a security parameter index (SPI) and subnet for the device, use the **cts l3 spi** command. To remove the mapping to an IPv4 subnet, use the **no** form of this command.

ctsl3 **spi A.B.C.D** / *length*

no ctsl3 **spi A.B.C.D** / *length*

Syntax Description

spi-number	SPI for the device. The range is from 0 to 429496729.
A.B.C.D/length	IPv4 subnet.

Command Default

None

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 Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure Layer 3 Cisco TrustSec global mapping for an SPI and subnet:

```
switch# config t
switch(config)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to remove Layer 3 global mapping for a subnet:

```
switch# config t
switch(config)# no cts l3 spi 10.10.1.1/23
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 mapping	Displays the Layer 3 Cisco TrustSec mapping for SPI values to IPv4 subnets.

cts l3 spi (interface)

To enable Layer 3 Cisco TrustSec and configure a security parameter index (SPI) on an interface, use the **cts l3 spi** command. To revert to the default, use the **no** form of this command.

cts l3 spi *spi-number*

no cts l3

Syntax Description

spi-number	SPI for the interface. The range is from 0 to 429496729.

Command Default

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 Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to disable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts l3
```

Related Commands

Command	Description
cts l3 spi (global)	Enables the Layer 3 Cisco TrustSec for the device.
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 interface	Displays the Layer 3 Cisco TrustSec configuration on the interfaces.

cts l3 spi (interface)

To enable Layer 3 Cisco TrustSec and configure a security parameter index (SPI) on an interface, use the **cts l3 spi** command. To revert to the default, use the **no** form of this command.

cts l3 spi *spi-number*

no cts l3

Syntax Description

spi-number	SPI for the interface. The range is from 0 to 429496729.

Command Default

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 Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts l3 spi 3 10.10.1.1/23
```

This example shows how to disable Layer 3 Cisco TrustSec for an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts l3
```

Related Commands

Command	Description
cts l3 spi (global)	Enables the Layer 3 Cisco TrustSec for the device.
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts l3 interface	Displays the Layer 3 Cisco TrustSec configuration on the interfaces.

cts manual

To enter Cisco TrustSec manual configuration for an interface, use the **cts manual** command. To remove the manual configuration, use the **no** form of this command.

cts manual

no cts manual

Syntax Description

This command has no arguments or keywords.

Command Default

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 Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to enter Cisco TrustSec manual configuration mode for an interface:

```
switch# configure terminal
switch(config)# interface etherent 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)#
```

This example shows how to remove the Cisco TrustSec manual configuration from an interface:

```
switch# configure terminal
switch(config)# interface etherent 2/4
switch(config-if)# no cts manual
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

Command	Description
show cts interface	Displays Cisco TrustSec configuration information for interfaces.

cts refresh environment-data

To refresh the Cisco TrustSec environment data downloaded from the AAA server, use the **cts refresh environment-data** command.

cts refresh environment-data

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

Ensure that you are using the Cisco Identity Services Engine (ISE) Release 1.0 or later releases.

Examples

This example shows how to refresh the Cisco TrustSec environment data downloaded from the AAA server:

```
switch# cts refresh environment-data
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts environment-data	Displays the Cisco TrustSec environment data.

cts refresh role-based-policy

To refresh the Cisco TrustSec security group access control list (SGACL) policies downloaded from the Cisco Secure ACS, use the **cts refresh role-based-policy** command.

cts refresh role-based-policy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enter Cisco TrustSec manual configuration mode for an interface:

```
switch# cts refresh role-based-policy
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays Cisco TrustSec SGACL policy configuration.

cts rekey

To rekey an interface for Cisco TrustSec policies, use the **cts rekey** command.

cts rekey ethernet *slot/port*

Syntax Description

ethernet *slot*/*port*	Specifies an Ethernet interface.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to rekey an interface for Cisco TrustSec:

```
switch# cts rekey ethernet 2/3
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays Cisco TrustSec configuration information for interfaces.

cts role-based access-list

To create or specify a Cisco TrustSec security group access control list (SGACL) and enter role-based access control list configuration mode, use the **cts role-based access-list** command. To remove an SGACL, use the **no** form of this command.

cts role-based access-list *list-name*

no cts role-based access-list *list-name*

Syntax Description

list-name	Name for the SGACL. The name is alphanumeric and case-sensitive. The maximum length is 32 characters.

Command Default

None

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 Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to create a Cisco TrustSec SGACL and enter role-based access list configuration mode :

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)#
```

This example shows how to remove a Cisco TrustSec SGACL:

```
switch# configure terminal
switch(config)# no cts role-based access-list MySGACL
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

cts role-based counters enable

To enable role-based access control list (RBACL) statistics, use the **cts role-based counters enable** command. To disabled RBACL statistics, use the **no** form of this command.

cts role-based counters enable

no cts role-based counters enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

To use this command, you must enable RBACL policy enforcement on the VLAN and VRF.

When you enable RBACL statistics, each policy requires one entry in the . If you do not have enough space remaining in the , an error message appears, and you cannot enable the statistics.

When you modify an RBACL policy, statistics for the previously assigned access control entry (ACE) are displayed, and the newly assigned ACE statistics are initialized to 0.

RBACL statistics are lost only when the Cisco NX-OS device reloads or you deliberately clear the statistics.

This command requires the Advanced Services license.

Examples

This example shows how to enable RBACL statistics:

```
switch# configure terminal
switch(config)# cts role-based counters enable
```

This example shows how to disable RBACL statistics:

```
switch# configure terminal
switch(config)# no cts role-based counters enable
```

Related Commands

Command	Description
clear cts role-based counters	Clears the RBACL statistics so that all counters are reset to 0.
show cts role-based counters	Displays the configuration status of RBACL statistics and lists statistics for all RBACL policies.

cts role-based detailed-logging

To enable the displaying of ACE-Action details for the RBACL policies, use the **cts role-based detailed-logging** command. To revert to the default, use the **no** form of this command.

cts role-based detailed-logging

no cts role-based detailed-logging

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configurationVRF configuration

Command History

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

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

Note To view the detailed ACLLOGS, you need to enable logging ip access-list detailed after enabling **cts role-based detailed logging**.

Examples

This example shows how to configure RBACL ace level permission and monitor logging:

```
switch# configure terminal
switch(config)# cts role-based detailed-logging
```

This example shows how to disable RBACL ace level permission and monitor logging:

```
switch# configure terminal
switch(config)# no
cts role-based detailed-logging
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based enable	Displays the Cisco TrustSec SGACL policy enforcement configuration.

cts role-based enforcement

To enable Cisco TrustSec security group access control list (SGACL) enforcement in a VLAN or Virtual Routing and Forwarding instance (VRF), use the **cts role-based enforcement** command. To revert to the default, use the **no** form of this command.

To disable Cisco TrustSec SGACL enforcement in an L3 interface or L3 port-channel, use the **no cts role-based enforcement** command. To revert to the default, use the **cts role-based enforcement** command.

cts role-based enforcement

no cts role-based enforcement

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled for VLAN, and Virtual Routing and Forwarding instance (VRF).

Enabled for L3 interfaces and L3 port-channels.

Command Modes

Global configuration VLAN configuration VRF configuration Interface configuration

Command History

Release	Modification
8.0(1)	Added the support for disabling SGACL policy enforcement on L3 interfaces and L3 port-channels.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable Cisco TrustSec SGACL enforcement in the default VRF:

```
switch# configure terminal
switch(config)# cts role-based enforcement
```

This example shows how to enable Cisco TrustSec SGACL enforcement in a VLAN:

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# cts role-based enforcement
```

This example shows how to enable Cisco TrustSec SGACL enforcement in a nondefault VRF:

```
switch# configure terminal
switch(config)# vrf context MyVRF
switch(config-vrf)# cts role-based enforcement
```

This example shows how to disable Cisco TrustSec SGACL enforcement in an interface and L3 port-channel:

```
switch# configure terminal
switch(config)# interface ethernet 6/2
switch(config-if)# no cts role-based enforcement
switch(config-if)# exit


switch(config)# interface port-channel 100
switch(config-if)# no cts role-based enforcement
switch(config-if)# exit
```

This example shows how to disable Cisco TrustSec SGACL enforcement:

```
switch# configure terminal
switch(config)# no cts role-based enforcement
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based enable	Displays the Cisco TrustSec SGACL policy enforcement configuration.

cts role-based monitor

To configure RBACL monitor, use the **cts role-based monitor** command. To revert to the default, use the **no** form of this command.

cts role-based monitor {**all**| **enable**| **permissions from**| {**sgt**| **unknown** }| **to** | {**dgt**| **unknown**}}[*ipv4* | *ipv6*]

no cts role-based monitor {**all**| **enable**| **permissions from**| {**sgt**| **unknown** }| **to** | {**dgt**| **unknown**}}[*ipv4* | *ipv6*]

Syntax Description

all	Enables monitoring permissions for all source groups to all destination groups.
enable	Enables RBACL monitor mode.
permission	Specifies the range for the SGT and DGT that needs to be monitored.
sgt	Specifies any SGT.
dgt	Specifies the Specifies the destination SGT.
unknown	Specifies an unknown SGT.
ipv4	Specifies the IPv4 protocol version.
ipv6	Specifies the IPv6 protocol version.

Command Default

Disabled

Command Modes

Global configurationVRF configuration

Command History

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

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

Examples

This example shows how to enable monitoring permissions for all source groups to all destination groups:

```
switch# configure terminal
switch(config)# cts role-based monitor all
```

This example shows how to disable monitoring permissions for all source groups to all destination groups:

```
switch# configure terminal
switch(config)# no cts role-based monitor all
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based enable	Displays the Cisco TrustSec SGACL policy enforcement configuration.

cts role-based policy priority-static

To set a higher install priority for the SGACLs configured by using CLI, use the **cts role-based policy priority-static** command. Use the **no** form of this command to revert, that is, set the install priority for the SGACLs downloaded by ISE.

cts role-based policy priority-static

no cts role-based policy priority-static

Command Default

Install priority is set for the SGACLs configured by using CLI.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

Examples

This example shows how to set higher install priority for ISE configured SGACLs:

```
switch# configure terminal
switch(config)# no cts role-based policy priority-static
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
cts refresh role-based-policy	Refreshes the Cisco TrustSec security group access control list (SGACL) policies.
show cts role-based policy	Displays the Cisco TrustSec SGACL policies and their details.

cts role-based sgt

To manually configure mapping of Cisco TrustSec security group tags (SGTs) to a security group access control list (SGACL), use the **cts role-based sgt** command. To remove the SGT mapping to an SGACL, use the **no** form of this command.

cts role-based sgt {**sgt-value**| **any**| **unknown**} **dgt** {**dgt-value**| **unknown**} **access-list list-name**

no cts role-based sgt {*sgt-value*| **any**| **unknown**} **dgt** {*dgt-value*| **unknown**}

Syntax Description

sgt-value	Source SGT value. The range is 0 to 65533.
any	Specifies any SGT.
unknown	Specifies an unknown SGT.
dgt	Specifies the destination SGT.
dgt-value	Destination SGT value. The range is 0 to 65533.
access-list *list-name*	Specifies the name for the SGACL.

Command Default

None

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 Cisco TrustSec feature using the **feature cts** command.

You must configure the SGACL before you can configure SGT mapping.

This command requires the Advanced Services license.

Examples

This example shows how to configure SGT mapping for an SGACL:

```
switch# configure terminal
switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL
```

This example shows how to remove SGT mapping for an SGACL

```
switch# configure terminal
switch(config)# no cts role-based sgt 3 sgt 10
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based policy	Displays the Cisco TrustSec SGT mapping for an SGACL.

cts sxp allow default-route-sgt

To enable the default route for SGT bindings, use the **cts sxp allow default-route-sgt** command. To disable, use the **no** form of this command.

cts sxp allow default-route-sgt

no cts sxp allow default-route-sgt

Syntax Description

This command has no arguments or keywords.

Command Default

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 Cisco TrustSec SXP feature using the **cts sxp enable** command.

Examples

This example shows how to expand the network limit:

```
switch# configure terminal
switch(config)# cts sxp allow default-route-sgt
```

This example shows how to disable the network limit:

```
switch# configure terminal
switch(config)# no cts sxp allow default-route-sgt
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp connection peer

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) peer connection for Cisco TrustSec, use the **cts sxp connection peer** command. To remove the SXP connection, use the **no** form of this command.

cts sxp connection peer *ipv4-address* **[source***source-ip-address* **password** {**default| none| required**} **mode** {**local| peer**} [[[**listener| speaker**] [**hold-time** *minimum-time maximum-time*]]| **both** [**vrf** *vrf-name*]]

no cts sxp connection peer *ipv4-address* {**source| password**} {**default| none**} **mode** {**local| peer**} [[[**listener| speaker**] [**hold-time** *minimum-time maximum-time*| **vrf** *vrf-name*]]| **both** [**vrf** *vrf-name*]]

Syntax Description

peer-ipv4-addr	IPv4 address of the peer device.
source *src-ipv4-addr*	(Optional) Specifies the IPv4 address of the source device.
password	Specifies the password option to use for the SXP authentication.
default	Specifies that SXP should use the default SXP password for the peer connection.
none	Specifies that SXP should not use a password.
required	Specifies the password that SXP should use for this peer connection.
password	Clear text password. The password is alphanumeric and case-sensitive. The maximum length is 32 characters.
7 *encrypted password*	Specifies an encrypted password. The maximum length is 32 characters.
mode	Specifies the mode of the peer device.
speaker	Specifies that the peer is the speaker.
listener	Specifies that the peer is the listener.
vrf *vrf-name*	(Optional) Specifies the VRF for the peer.

hold-time *minimum-time maximum-time*	(Optional) Specifies the hold-time period, in seconds, for the device. The range for minimum and maximum time is from 0 to 65535. A *maximum-time* value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a *minimum-time* value is required. **Note** If both minimum and maximum times are required, the *maximum-time* value must be greater than or equal to the *minimum-time* value.

Command Default

The CTS-SXP peer IP address is not configured and no CTS-SXP peer password is used for the peer connection.

The default setting for a CTS-SXP connection password is **none**.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was modified. The **hold-time** keyword and *minimum-time* and *maximum-time* arguments were added.
4.1(3)	Added the **7** option to allow encrypted passwords.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

If you do not specify a source IPv4 address, you must configure a default SXP source IPv4 address using the **cts sxp default source-ip** command.

If you specify default as the password mode, you must configure a default SXP password using the **cts sxp default password** command.

This command requires the Advanced Services license.

Examples

This example shows how to configure an SXP peer connection:

```
switch# configure terminal
switch(config)# cts sxp connection peer 10.10.1.1 source 10.10.2.2 password default mode
listener
```

This example shows how to remove an SXP peer connection:

```
switch# configure terminal
switch(config)# no cts sxp connection peer 10.10.1.1
```

This example shows how to configure the hold-time for the SXPv4 protocol for each connection.

```
switch# configure terminal
switch(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
hold-time 500
```

Related Commands

Command	Description
cts sxp default password	Configures the default SXP password for the device.
cts sxp default source-ip	Configures the default SXP source IPv4 address for the device.
feature cts	Enables the Cisco TrustSec feature.
show cts sxp connection	Displays the Cisco TrustSec SXP peer connection information.

cts sxp default password

To configure the default Security Group Tag (SGT) Exchange Protocol (SXP) password for the device, use the **cts sxp default password** command. To remove the default, use the **no** form of this command.

cts sxp default password {*password*| **7** *encrypted-password*}

no cts sxp default password

Syntax Description

password	Clear text password. The password is alphanumeric and case-sensitive. The maximum length is 32 characters.
7 *encrypted password*	Specifies an encrypted password. The maximum length is 32 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(3)	Added the **7** option to allow encrypted passwords.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to configure the default SXP password for the device:

```
switch# configure terminal
switch(config)# cts sxp default password Cisco654
```

This example shows how to remove the default SXP password:

```
switch# configure terminal
switch(config)# no cts sxp default password
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp default source-ip

To configure the default Security Group Tag (SGT) Exchange Protocol (SXP) source IPv4 address for the device, use the **cts sxp default source-ip** command. To revert to the default, use the **no** form of this command.

cts sxp default source-ip *ipv4-address*

no cts sxp default source-ip *ipv4-address*

Syntax Description

ipv4-address	Default SXP IPv4 address for the device.

Command Default

None

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 Cisco TrustSec feature using the **feature cts** command.

You can use only IPv4 addressing with Cisco TrustSec.

This command requires the Advanced Services license.

Examples

This example shows how to configure the default SXP source IP address for the device:

```
switch# configure terminal
switch(config)# cts sxp default source-ip 10.10.3.3
```

This example shows how to remove the default SXP source IP address:

```
switch# configure terminal
switch(config)# no cts sxp default source-ip
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp enable

To enable the Security Group Tag (SGT) Exchange Protocol (SXP) peer on a device, use the **cts sxp enable** command. To revert to the default, use the **no** form of this command.

cts sxp enable

no cts sxp enable

Syntax Description

This command has no arguments or keywords.

Command Default

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 Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to enable SXP:

```
switch# configure terminal
switch(config)# cts sxp enable
```

This example shows how to disable SXP:

```
switch# configure terminal
switch(config)# no cts sxp enable
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp listener hold-time

To configure the global hold-time period of a listener network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp listener hold-time** command in global configuration mode. To remove the hold time from the listener device, use the **no** form of this command.

cts sxp listener hold-time *minimum-period maximum-period*

no cts sxp listener hold-time

Syntax Description

minimum-period	Minimum allowed hold time in seconds. The range is from 1 to 65534.
maximum-period	Specifies the maximum allowed hold-time in seconds. The range is from 1 to 65534 seconds. **Note** The *maximum-period* specified must be greater than or equal to the *minimum-period*.

Command Default

The default hold time range for a listener device is 90 seconds to 180 seconds.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

SXP uses a TCP-based, keepalive mechanism to determine if a connection is live. SXPv4 adds an optional negotiated keepalive mechanism, the hold-time period, in order to provide more predictable and timely detection of connection loss.

Hold time can be configured globally on a network device. This global configuration will apply the configuration to all SXP connections configured on the device.

You may configure a hold-time period locally on a listener device or a default of 90 seconds to 180 seconds is used. A value of “0xFFFF..0xFFFF” indicates that the keepalive mechanism is not used.

The hold-time negotiation between the speaker device and the listener device succeeds when the speaker’s minimum acceptable hold-time falls below or within the desirable hold-time range of the listener. (Use the **cts sxp speaker hold-time** command to configure the hold-time of the speaker device.) If one end turns off the keepalive mechanism, the other end should also turn it off to make the negotiation successful.

The negotiation fails when the speaker's minimum acceptable hold-time is greater than the upper bound of the listener's hold-time range.

The selected hold-time period of a successful negotiation is the maximum of the speaker’s minimum acceptable hold-time and the lower bound of the listener’s hold-time range.

The speaker calculates the keepalive time to one-third of the selected hold time by default, unless a different keepalive time is locally configured.

Examples

The following example shows how to configure the hold time period of a listener device for a minimum of 300 seconds and a maximum of 500 seconds:

```
switch# configure terminal
switch(config)# cts sxp listener hold-time 300 500
```

Related Commands

Command	Description
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp speaker hold-time	Configures the hold time of a speaker device in an SXPv4 network.
show cts sxp	Displays the status of all Cisco TrustSec SXP configurations.

cts sxp mapping network-map

To expand the network limit, use the **cts sxp mapping network-map** command. To revert to the default, use the **no** form of this command.

cts sxp mapping network-map *num_bindings*

no cts sxp mapping network-map *num_bindings*

Syntax Description

num_bindings	Number of bindings to be expanded. The range is from 0 to 65535.

Command Default

Zero (0)

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 Cisco TrustSec feature by using the **feature cts** command.

Examples

This example shows how to expand the network limit:

```
switch# configure terminal
switch(config)# cts sxp mapping network-map 64
```

This example shows how to disable the network limit:

```
switch# configure terminal
switch(config)# no cts sxp mapping network-map 64
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp	Displays the Cisco TrustSec SXP configuration information.

cts sxp node-id

To configure the node ID of a network device for Cisco TrustSec (CTS) Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4), use the **cts sxp node-id** command in global configuration mode. To remove the node ID, use the **no** form of this command.

cts sxp node-id {*node-id* | **interface** *interface-type* | *ipv4-address*}

no cts sxp node-id

Syntax Description

node-id	Specifies the node ID of the device. Enter the node ID in hexadecimal format.
interface *interface-type*	Specifies the type of interface.
ipv4-address	Specifies the SXP peer IPv4 address.

Command Default

A node ID is not configured.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **cts sxp node-id** command configures the node ID of a network device.

An SXP node ID is used to identify the individual devices within the network. The node ID is a four-octet integer that can be configured by the user. If it is not configured by the user, SXP picks a node ID itself using the highest IPv4 address in the default VRF domain, in the same manner that EIGRP generates its node ID.

The node ID has to be unique in the network that SXP connections traverse to enable SXP loop prevention.

The SXP loop detection mechanism drops the binding propagation packets based on finding its own node ID in the peer sequence attribute. Changing a node ID in a loop detection running SXP network could break SXP loop detection functionality and therefore needs to be handled carefully.

Wait until the SXP bindings that are propagated with the particular node ID in the path attribute are deleted, before you change the node ID.

Note A syslog is generated when you change the node ID.

Examples

```
switch(config)# cts sxp node-id 172.16.1.3
```

Related Commands

Command	Description
cts sxp enable	Enables CTS-SXP on a device.
show cts sxp	Displays the status of all CTS-SXP configurations.

cts sxp reconcile-period

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) reconcile period timer, use the **cts sxp reconcile-period** command. To revert to the default, use the **no** form of this command.

cts sxp reconcile-period *seconds*

no cts sxp reconcile-period

Syntax Description

seconds	Number of seconds. The range is from 0 to 64000.

Command Default

60 seconds (1 minute)

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 Cisco TrustSec feature using the **feature cts** command.

After a peer terminates an SXP connection, an internal hold down timer starts. If the peer reconnects before the internal hold down timer expires, the SXP reconcile period timer starts. While the SXP reconcile period timer is active, the Cisco NX-OS software retains the SGT mapping entries learned from the previous connection and removes invalid entries.

Note Setting the SXP reconcile period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

This command requires the Advanced Services license.

Examples

This example shows how to configure the SXP reconcile period:

```
switch# configure terminal
switch(config)# cts sxp reconcile-period 120
```

This example shows how to revert to the default SXP reconcile period value:

```
switch# configure terminal
switch(config)# no cts sxp reconcile-period
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp connection	Displays the Cisco TrustSec SXP configuration information.

cts sxp retry-period

To configure a Security Group Tag (SGT) Exchange Protocol (SXP) retry period timer, use the **cts sxp retry-period** command. To revert to the default, use the **no** form of this command.

cts sxp retry-period *seconds*

no cts sxp retry-period

Syntax Description

seconds	Number of seconds. The range is from 0 to 64000.

Command Default

120 seconds (2 minutes)

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 Cisco TrustSec feature using the **feature cts** command.

The SXP retry period determines how often the Cisco NX-OS software retries an SXP connection. When an SXP connection is not successfully set up, the Cisco NX-OS software makes a new attempt to set up the connection after the SXP retry period timer expires.

Note Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

This command requires the Advanced Services license.

Examples

This example shows how to configure the SXP retry period:

```
switch# configure terminal
switch(config)# cts sxp retry-period 120
```

This example shows how to revert to the default SXP retry period value:

```
switch# configure terminal
switch(config)# no cts sxp retry-period
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts sxp connection	Displays the Cisco TrustSec SXP peer connection information.

cts sxp speaker hold-time

To configure the global hold-time period of a speaker network device in a Cisco TrustSec Security Group Tag (SGT) Exchange Protocol version 4 (SXPv4) network, use the **cts sxp speaker hold-time** command in global configuration mode. To remove the hold time from the speaker device, use the **no** form of this command.

cts sxp speaker hold-time *minimum-period*

no cts sxp speaker hold-time

Syntax Description

minimum-period	Minimum allowed hold time in seconds. The range is from 1 to 65534.

Command Default

The default hold time for a speaker device is 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The Security Group Tag Exchange Protocol (SXP) uses a TCP-based, keepalive mechanism to determine if a connection is live. SXPv4 adds an optional negotiated keepalive mechanism, the hold-time period, in order to provide more predictable and timely detection of connection loss.

Hold time can be configured globally on a network device. This global configuration will apply the configuration to all SXP connections configured on the device.

You may configure a hold-time period locally on a speaker device or a default of 120 seconds is used. This is the shortest period of time a speaker is willing to send keepalive messages for keeping the connection active. Any shorter hold-time period would require a faster keepalive rate than the rate the speaker is ready to support. A value of 0xFFFF indicates that the keepalive mechanism is not used.

The hold-time negotiation between the speaker device and the listener device succeeds when the speaker's minimum acceptable hold time falls below or within the desirable hold-time range of the listener. (Use the **cts sxp listener hold-time** command to configure the hold time of the listener device.) If one end turns off the keepalive mechanism, the other end should also turn it off to make the negotiation successful.

The negotiation fails when the speaker's minimum acceptable hold-time is greater than the upper bound of the listener's hold-time range.

The selected hold-time period of a successful negotiation is the maximum of the speaker's minimum acceptable hold time and the lower bound of the listener's hold-time range.

The speaker calculates the keepalive time to one-third of the selected hold time by default, unless a different keepalive time is locally configured.

Examples

The following example shows how to configure the minimum hold time period of a speaker device for 300 seconds:

```
switch(config)# cts sxp speaker hold-time 300
```

Related Commands

Command	Description
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp listener hold-time	Configures the hold time of a listener device in an SXPv4 network.
show cts sxp	Displays the status of all Cisco TrustSec SXP configurations.

D Commands

dot1x max-reauth-req

To change the maximum number of times that the Cisco NX-OS device retransmits reauthentication requests to supplicants on an interface before the session times out, use the **dot1x max-reauth-req** command. To revert to the default, use the **no** form of this command.

dot1x max-reauth-req *retry-count*

no dot1x max-reauth-req

Syntax Description

retry-count	Retry count for reauthentication requests. The range is from 1 to 10.

Command Default

2 retries

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to change the maximum number of reauthorization request retries for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-reauth-req 3
```

This example shows how to revert to the default maximum number of reauthorization request retries for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-reauth-req
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

Command	Description
show dot1x all	Displays all 802.1X information.

dot1x max-req

To change the maximum number of requests that the Cisco NX-OS device sends to a supplicant before restarting the 802.1X authentication, use the **dot1x max-req** command. To revert to the default, use the **no** form of this command.

dot1x max-req *retry-count*

no dot1x max-req

Syntax Description

retry-count	Retry count for request sent to supplicant before restarting 802.1X reauthentication. The range is from 1 to 10.

Command Default

Global configuration: 2 retries

Interface configuration: Global configuration setting

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to change the maximum number of request retries for the global 802.1X configuration:

```
switch# configure terminal
switch(config)# dot1x max-req 3
```

This example shows how to revert to the default maximum number of request retries for the global 802.1X configuration:

```
switch# configure terminal
switch(config)# no dot1x max-req
```

This example shows how to change the maximum number of request retries for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-req 4
```

This example shows how to revert to the default maximum number of request retries for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-req
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x pae authenticator

To create the 802.1X authenticator port access entity (PAE) role for an interface, use the **dot1x pae authenticator** command. To remove the 802.1X authenticator PAE role, use the **no** form of this command.

dot1x pae authenticator

no dot1x pae authenticator

Syntax Description

This command has no arguments or keywords.

Command Default

802.1X automatically creates the authenticator PAE when you enable the feature on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.

This command does not require a license.

Examples

This example shows how to create the 802.1X authenticator PAE role on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# dot1x pae authenticator
```

This example shows how to remove the 802.1X authenticator PAE role from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# no dot1x pae authenticator
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

Command	Description
show dot1x interface	Displays 802.1X feature status information for an interface.

dot1x port-control

To control the 802.1X authentication performed on an interface, use the **dot1x port-control** command. To revert to the default, use the **no** form of this command.

dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

no dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

Syntax Description

auto	Enables 802.1X authentication on the interface.
force-authorized	Disables 802.1X authentication on the interface and allows all traffic on the interface without authentication.
force-unauthorized	Disallows all authentication on the interface.

Command Default

force-authorized

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to change the 802.1X authentication action performed on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

This example shows how to revert to the default 802.1X authentication action performed on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x interface ethernet	Displays 802.1X information for an interface.

dot1x radius-accounting

To enable RADIUS accounting for 802.1X, use the **dot1x radius-accounting** command. To revert to the default, use the **no** form of this command.

dot1x radius-accounting

no dot1x radius-accounting

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to enable RADIUS accounting for 802.1X authentication:

```
switch# configure terminal
switch(config)# dot1x radius-accounting
```

This example shows how to disable RADIUS accounting for 802.1X authentication:

```
switch# configure terminal
switch(config)# no dot1x radius-accounting
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show running-config dot1x all	Displays all 802.1X information in the running configuration.

dot1x re-authentication (EXEC)

To manually reauthenticate 802.1X supplicants, use the **dot1x re-authentication** command.

dot1x reauthentication [**interface ethernet** *slot* | *port*]

Syntax Description

interface ethernet *slot/port*	(Optional) Specifies the interface for manual reauthentication.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to reauthenticate 802.1X supplicants manually:

```
switch# dot1x re-authentication
```

This example shows how to reauthenticate the 802.1X supplicant on an interface manually:

```
switch# dot1x re-authentication interface ethernet 2/1
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x re-authentication (global configuration and interface configuration)

To enable periodic reauthenticate of 802.1X supplicants, use the **dot1x re-authentication** command. To revert to the default, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

Global configuration: Disabled

Interface configuration: Global configuration setting

Command Modes

Global configurationInterface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

In global configuration mode, this command configures periodic reauthentication for all supplicants on the Cisco NX-OS device. In interface configuration mode, this command configures periodic reauthentication only for supplicants on the interface.

This command does not require a license.

Examples

This example shows how to enable periodic reauthentication of 802.1X supplicants:

```
switch# configure terminal
switch(config)# dot1x re-authentication
```

This example shows how to disable periodic reauthentication of 802.1X supplicants:

```
switch# configure terminal
switch(config)# no dot1x re-authentication
```

This example shows how to enable periodic reauthentication of 802.1X supplicants on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x re-authentication
```

This example shows how to disable periodic reauthentication of 802.1X supplicants on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x re-authentication
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x system-auth-control

To enable 802.1X authentication, use the **dot1x system-auth-control** command. To disable 802.1X authentication, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **dot1x system-auth-control** command does not delete the 802.1X configuration.

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to disable 802.1X authentication:

```
switch# configure terminal
switch(config)# no dot1x system-auth-control
```

This example shows how to enable 802.1X authentication:

```
switch# configure terminal
switch(config)# dot1x system-auth-control
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x	Displays 802.1X feature status information.

dot1x timeout quiet-period

To configure the 802.1X quiet-period timeout globally or for an interface, use the **dot1x timeout quiet-period** command. To revert to the default, use the **no** form of this command.

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Syntax Description

seconds	Number of seconds for the 802.1X quiet-period timeout. The range is from 1 to 65535.

Command Default

Global configuration: 60 seconds

Interface configuration: The value of the global configuration

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X quiet-period timeout is the number of seconds that the device remains in the quiet state following a failed authentication exchange with a supplicant.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the global 802.1X quiet-period timeout:

```
switch# configure terminal
switch(config)# dot1x timeout quiet-period 45
```

This example shows how to revert to the default global 802.1X quiet-period timeout:

```
switch# configure terminal
switch(config)# no dot1x timeout quiet-period
```

This example shows how to configure the 802.1X quiet-period timeout for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout quiet-period 50
```

This example shows how to revert to the default 802.1X quiet-period timeout for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x timeout quiet-period
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x timeout ratelimit-period

To configure the 802.1X rate-limit period timeout for the supplicants on an interface, use the **dot1x timeout ratelimit-period** command. To revert to the default, use the **no** form of this command.

dot1x timeout ratelimit-period *seconds*

no dot1x timeout ratelimit-period

Syntax Description

seconds	Number of seconds for the 802.1X rate-limit period timeout. The range is from 1 to 65535.

Command Default

0 seconds

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X rate-limit timeout period is the number of seconds that the authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated. This value overrides the global quiet period timeout.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the 802.1X rate-limit period timeout on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

This example shows how to revert to the default 802.1X rate-limit period timeout on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x interface ethernet	Displays 802.1X information for an interface.

dot1x timeout re-authperiod

To configure the 802.1X reauthentication-period timeout either globally or on an interface, use the **dot1x timeout re-authperiod** command. To revert to the default, use the **no** form of this command.

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

Syntax Description

seconds	Number of seconds for the 802.1X reauthentication-period timeout. The range is from 1 to 65535.

Command Default

Global configuration: 3600 seconds

Interface configuration: Global configuration setting

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X reauthentication timeout period is the number of seconds between reauthentication attempts.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the global 802.1X reauthentication-period timeout:

```
switch# configure terminal
switch(config)# dot1x timeout re-authperiod 3000
```

This example shows how to configure the 802.1X reauthentication-period timeout on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout re-authperiod 3300
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x timeout server-timeout

To configure the 802.1X server timeout for an interface, use the **dot1x timeout server-timeout** command. To revert to the default, use the **no** form of this command.

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Syntax Description

seconds	Number of seconds for the 802.1X server timeout. The range is from 1 to 65535.

Command Default

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X server timeout for an interface is the number of seconds that the Cisco NX-OS device waits before retransmitting a packet to the authentication server. This value overrides the global reauthentication period timeout.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the global 802.1X server timeout interval:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

This example shows how to revert to the default global 802.1X server timeout interval:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x interface ethernet	Displays 802.1X information for an interface.

dot1x timeout supp-timeout

To configure the 802.1X supplicant timeout for an interface, use the **dot1x timeout supp-timeout** command. To revert to the default, use the **no** form of this command.

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Syntax Description

seconds	Number of seconds for the 802.1X supplicant timeout. The range is from 1 to 65535.

Command Default

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X supplicant timeout for an interface is the number of seconds that the Cisco NX-OS device waits for the supplicant to respond to an EAP request frame before the Cisco NX-OS device retransmits the frame.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the 802.1X server timeout interval on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout supp-timeout 45
```

This example shows how to revert to the default 802.1X server timeout interval on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x timeout supp-timeout
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x interface ethernet	Displays 802.1X information for an interface.

dot1x timeout tx-period

To configure the 802.1X transmission-period timeout either globally or for an interface, use the **dot1x timeout tx-period** command. To revert to the default, use the **no** form of this command.

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

Syntax Description

seconds	Number of seconds for the 802.1X transmission-period timeout. The range is from 1 to 65535.

Command Default

Global configuration: 60 seconds

Interface configuration: Global configuration setting

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The 802.1X transmission-timeout period is the number of seconds that the Cisco NX-OS device waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request.

You must use the **feature dot1x** command before you configure 802.1X.

Note You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

This command does not require a license.

Examples

This example shows how to configure the global 802.1X transmission-period timeout:

```
switch# configure terminal
switch(config)# dot1x timeout tx-period 45
```

This example shows how to revert to the default global 802.1X transmission-period timeout:

```
switch# configure terminal
switch(config)# no dot1x timeout tx-period
```

This example shows how to configure the 802.1X transmission-period timeout for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout tx-period 45
```

This example shows how to revert to the default 802.1X transmission-period timeout for an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x timeout tx-period
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

deadtime

To configure the dead-time interval for a RADIUS or TACACS+ server group, use the **deadtime** command. To revert to the default, use the **no** form of this command.

deadtime *minutes*

no deadtime *minutes*

Syntax Description

minutes	Number of minutes for the interval. The range is from 0 to 1440 minutes. **Note** Setting the dead-time interval to 0 disables the timer.

Command Default

0 minutes

Command Modes

RADlUS server group configuration TACACS+ server group configuration

Command History

Release	Modification
4.0(1)	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 set the dead-time interval to 2 minutes for a RADIUS server group:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

This example shows how to set the dead-time interval to 5 minutes for a TACACS+ server group:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
```

This example shows how to revert to the dead-time interval default:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
feature tacacs+	Enables TACACS+.
tacacs-server host	Configures a TACACS+ server.

delete ca-certificate

To delete certificate authority certificates, use the **delete ca-certificate** command.

delete ca-certificate

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command deletes the CA certificate or certificate chain corresponding to the trustpoint CA. As a result, the trustpoint CA is no longer trusted. If there is an identity certificate form the CA, you must delete it before you can delete the CA certificate. This prevents the accidental deletion of a CA certificate when you have not yet deleted the identity certificate obtained from that CA. Deleting the CA certificate may be necessary when you no longer want to trust the CA because the CA is compromised or the CA certificate has expired.

The trustpoint configuration, certificates, and key pair configurations are persistent only after saving to the startup configuration. Deletions become persistent only after you save the running configuration to the startup configuration.

Enter the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

This command does not require a license.

Examples

This example shows how to delete a certificate authority certificate:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete ca-certificate
```

Related Commands

Command	Description
delete certificate	Deletes the identity certificate.
delete crl	Deletes the CRL from the trustpoint.

delete certificate

To delete the identity certificate, use the **delete certificate** command.

delete certificate [force]

Syntax Description

force	(Optional) Forces the deletion of the identity certificate.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use the **delete certificate** command to delete the identity certificate obtained from the trustpoint CA when the identity certificate expires or the corresponding key pair is compromised. Applications on the device are left without any identity certificate to use after you delete the last or the only identity certificate present. The Cisco NX-OS software generates an error message if the certificate being deleted is the only certificate present or is the last identity certificate in a chain. You can use the optional **force** keyword to remove the certificate.

The trustpoint configuration, certificates, and key pair configurations are persistent only after saving to the startup configuration. Deletions become persistent only after you save the running configuration to the startup configuration.

Enter the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

This command does not require a license.

Examples

This example shows how to delete the identity certificate:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate
```

This example shows how to force the deletion of the identity certificate:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate force
```

Related Commands

Command	Description
delete ca-certificate	Deletes the certificate authority certificate.
delete crl	Deletes the CRL from the trustpoint.

delete crl

To delete the certificate revocation list (CRL) from the trustpoint, use the **delete crl** command.

delete crl

Syntax Description

This command has no argument or keywords.

Command Default

None

Command Modes

Trustpoint 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 delete the CRL from the trustpoint:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete crl
```

Related Commands

Command	Description
delete ca-certificate	Deletes the certificate authority certificate.
delete certificate	Deletes the identity certificate.

deny (ARP)

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

General Syntax

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

[*sequence-number*] **deny request ip** {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

[*sequence-number*] **deny response ip** {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} {**any**| **host** *target-IP*| *target-IP target-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} [**any**| **host** *target-MAC*| *target-MAC target-MAC-mask*] **[log]**

no *sequence-number*

no deny ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

no deny request ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

no deny response ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} {**any**| **host** *target-IP*| *target-IP target-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} [**any**| **host** *target-MAC*| *target-MAC target-MAC-mask*] **[log]**

Syntax Description

sequence-number	(Optional) Sequence number of the **deny** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
ip	Introduces the IP address portion of the rule.

any	(Optional) Specifies that any host matches the part of the rule that contains the **any** keyword. You can use the **any** to specify the sender IP address, target IP address, sender MAC address, and target MAC address.
host *sender-IP*	(Optional) Specifies that the rule matches ARP packets only when the sender IP address in the packet matches the value of the *sender-IP* argument. Valid values for the *sender-IP* argument are IPv4 addresses in dotted-decimal format.
sender-IP sender-IP-mask	(Optional) IPv4 address and mask for the set of IPv4 addresses that the sender IP address in the packet can match. The *sender-IP* and *sender-IP-mask* argument must be given in dotted-decimal format. Specifying 255.255.255.255 as the *sender-IP-mask* argument is the equivalent of using the **host** keyword.
mac	Introduces the MAC address portion of the rule.
host *sender-MAC*	(Optional) Specifies that the rule matches ARP packets only when the sender MAC address in the packet matches the value of the *sender-MAC* argument. Valid values for the *sender-MAC* argument are MAC addresses in dotted-hexadecimal format.
sender-MAC sender-MAC-mask	(Optional) MAC address and mask for the set of MAC addresses that the sender MAC address in the packet can match. The *sender-MAC* and *sender-MAC-mask* argument must be given in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the *sender-MAC-mask* argument is the equivalent of using the **host** keyword.
log	(Optional) Specifies that the device logs ARP packets that match the rule.
request	(Optional) Specifies that the rule applies only to packets containing ARP request messages. **Note** If you omit both the **request** and the **response** keywords, the rule applies to all ARP messages.
response	(Optional) Specifies that the rule applies only to packets containing ARP response messages. **Note** If you omit both the **request** and the **response** keywords, the rule applies to all ARP messages.

host *target-IP*	(Optional) Specifies that the rule matches ARP packets only when the target IP address in the packet matches the value of the *target-IP* argument. You can specify **host** *target-IP* only when you use the **response** keyword. Valid values for the *target-IP* argument are IPv4 addresses in dotted-decimal format.
target-IP target-IP-mask	(Optional) IPv4 address and mask for the set of IPv4 addresses that the target IP address in the packet can match. You can specify *target-IP target-IP-mask* only when you use the **response** keyword. The *target-IP* and *target-IP-mask* argument must be given in dotted-decimal format. Specifying 255.255.255.255 as the *target-IP-mask* argument is the equivalent of using the **host** keyword.
host *target-MAC*	(Optional) Specifies that the rule matches ARP packets only when the target MAC address in the packet matches the value of the *target-MAC* argument. You can specify **host** *target-MAC* only when you use the **response** keyword. Valid values for the *target-MAC* argument are MAC addresses in dotted-hexadecimal format.
target-MAC target-MAC-mask	(Optional) MAC address and mask for the set of MAC addresses that the target MAC address in the packet can match. You can specify *target-MAC target-MAC-mask* only when you use the **response** keyword. The *target-MAC* and *target-MAC-mask* argument must be given in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the *target-MAC-mask* argument is the equivalent of using the **host** keyword.

Command Default

None

Command Modes

ARP ACL configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A newly created ARP ACL contains no rules.

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

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

If you do not specify either the **response** or **request** keyword, the rule applies to packets that contain any ARP message.

This command does not require a license.

Examples

This example shows how to enter ARP access list configuration mode for an ARP ACL named arp-acl-01 and add a rule that denies ARP request messages that contain a sender IP address that is within the 10.32.143.0 subnet:

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)# deny request ip 10.32.143.0 255.255.255.0 mac any
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip arp inspection filter	Applies an ARP ACL to a VLAN.
permit (ARP)	Configures a permit rule in an ARP ACL.
remark	Configures a remark in an ACL.
show arp access-list	Displays all ARP ACLs or one ARP ACL.

deny (IPv4)

To create an IPv4 ACL rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no deny *protocol source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*| *icmp-type* [*icmp-code*]] [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Group Management Protocol

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Protocol v4

[*sequence-number*] **deny ip** *source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [*flags*] **[established]** [**packet-length** *operator packet-length* [*packet-length*]]

User Datagram Protocol

[*sequence-number*] **deny udp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*| **precedence** *precedence*] **[fragments] [log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Syntax Description

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

dscp *dscp*	

(Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords:

- 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010.
- **af11—**Assured Forwarding (AF) class 1, low drop probability (001010)
- **af12—**AF class 1, medium drop probability (001100)
- **af13—**AF class 1, high drop probability (001110)
- **af21—**AF class 2, low drop probability (010010)
- **af22—**AF class 2, medium drop probability (010100)
- **af23—**AF class 2, high drop probability (010110)
- **af31—**AF class 3, low drop probability (011010)
- **af32—**AF class 3, medium drop probability (011100)
- **af33—**AF class 3, high drop probability (011110)
- **af41—**AF class 4, low drop probability (100010)
- **af42—**AF class 4, medium drop probability (100100)
- **af43—**AF class 4, high drop probability (100110)
- **cs1—**Class-selector (CS) 1, precedence 1 (001000)
- **cs2—**CS2, precedence 2 (010000)
- **cs3—**CS3, precedence 3 (011000)
- **cs4—**CS4, precedence 4 (100000)
- **cs5—**CS5, precedence 5 (101000)
- **cs6—**CS6, precedence 6 (110000)

	• **cs7—**CS7, precedence 7 (111000) • **default—**Default DSCP value (000000) • **ef—**Expedited Forwarding (101110)
precedence *precedence*	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword, as follows: • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. • **critical—**Precedence 5 (101) • **flash—**Precedence 3 (011) • **flash-override—**Precedence 4 (100) • **immediate—**Precedence 2 (010) • **internet—**Precedence 6 (110) • **network—**Precedence 7 (111) • **priority—**Precedence 1 (001) • **routine—**Precedence 0 (000)
fragments	(Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: • Whether the protocol was TCP, UDP, ICMP or a number • Source and destination addresses • Source and destination port numbers, if applicable

time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command. The *time-range-name* argument can be up to 64 alphanumeric, case-sensitive characters.
icmp-message	(ICMP only: Optional) ICMP message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMP Message Types” in the “Usage Guidelines” section.
icmp-type [*icmp-code*]	(ICMP only: Optional) ICMP message type that the rule matches. Valid values for the *icmp-type* argument are an integer from 0 to 255. If the ICMP message type supports message codes, you can use the *icmp-code* argument to specify the code that the rule matches. For more information about ICMP message types and codes, see http://www.iana.org/assignments/icmp-parameters .
igmp-message	(IGMP only: Optional) IGMP message type that the rule matches. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp—**Distance Vector Multicast Routing Protocol • **host-query—**Host query • **host-report—**Host report • **pim—**Protocol Independent Multicast • **trace—**Multicast trace

operator port [*port*]	(Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the port in the packet is equal to the *port* argument. • **gt—**Matches only if the port in the packet is greater than and not equal to the *port* argument. • **lt—**Matches only if the port in the packet is less than and not equal to the *port* argument. • **neq—**Matches only if the port in the packet is not equal to the *port* argument. • **range—**Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port object group specified by the *portgroup* argument, which can be up to 64 alphanumeric, case-sensitive characters. Whether the IP port object group applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port object groups.

flags	(TCP only; Optional) TCP control bit flags that the rule matches. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.
packet-length*operatorpacket-length* [*packet-length*	(Optional) Rule matches only packets that have a length in bytes that satisfies the condition specified by the *operator* and *packet-length* arguments. Valid values for the *packet-length* argument are whole numbers from 20 to 9210. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the packet length in bytes is equal to the *packet-length* argument. • **gt—**Matches only if the packet length in bytes is greater than the *packet-length* argument. • **lt**—Matches only if the packet length in bytes is less than the *packet-length* argument. • **neq—**Matches only if the packet length in bytes is not equal to the *packet-length* argument. • **range—**Requires two *packet-length* arguments and matches only if the packet length in bytes is equal to or greater than the first *packet-length* argument and equal to or less than the second *packet-length* argument.

Command Default

A newly created IPv4 ACL contains no rules.

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

Command Modes

IPv4 ACL configuration

Command History

Release	Modification
4.1(2)	Support was added for the following: • The **ahp**, **eigrp**, **esp**, **gre**, **nos**, **ospf**, **pcp**, and **pim** protocol keywords. • The **packet-length** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

When the device applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

This command does not require a license.

Protocol

You can specify the protocol of packets that the rule applies to by the protocol name or the number of the protocol. If you want the rule to apply to all IPv4 traffic, use the **ip** keyword.

The protocol keyword that you specify affects the additional keywords and arguments that are available. Unless otherwise specified, only the other keywords that apply to all IPv4 protocols are available. Those keywords include the following:

-
  - **dscp**
  - **fragments**
  - **log**
  - **packet-length**
  - **precedence**
  - **time-range**

Valid protocol numbers are from 0 to 255.

Valid protocol names are the following keywords:

- **ahp—**Specifies that the rule applies to authentication header protocol (AHP) traffic only.
- **eigrp—**Specifies that the rule applies to Enhanced Interior Gateway Routing Protocol (EIGRP) traffic only.
- **esp—**Specifies that the rule applies to Encapsulating Security Protocol (ESP) traffic only.
- **gre—**Specifies that the rule applies to General Routing Encapsulation (GRE) traffic only.

- **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **igmp**—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **ip**—Specifies that the rule applies to all IPv4 traffic.
- **nos**—Specifies that the rule applies to KA9Q NOS-compatible IP-over-IP tunneling traffic only.
- **ospf**—Specifies that the rule applies to Open Shortest Path First (OSPF) traffic only.
- **pcp**—Specifies that the rule applies to payload compression protocol (PCP) traffic only.
- **pim**—Specifies that the rule applies to protocol-independent multicast (PIM) traffic only.
- **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.

Source and Destination

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

- IP address group object—You can use an IPv4 address group object to specify a *source* or *destination* argument. Use the **object-group ip address** command to create and change IPv4 address group objects. The syntax is as follows:

```
addrgroup

address-group-name
```

The following example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the *destination* argument:

```
switch(config-acl)# deny ip any addrgroup lab-gateway-svrs
```

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

```
IPv4-address network-wildcard
```

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

```
switch(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
```

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

```
IPv4-address/prefix-len
```

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

```
switch(config-acl)# deny udp 192.168.67.0/24 any
```

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

```
host
IPv4-address
```

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

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

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

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

ICMP Message Types

The *icmp-message* argument can be one of the following keywords:

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

- **information-request—**Information requests
- **mask-reply—**Mask replies
- **mask-request—**Mask requests
- **mobile-redirect—**Mobile host redirect
- **net-redirect—**Network redirect
- **net-tos-redirect—**Net redirect for ToS
- **net-tos-unreachable—**Network unreachable for ToS
- **net-unreachable—**Net unreachable
- **network-unknown—**Network unknown
- **no-room-for-option—**Parameter required but no room
- **option-missing—**Parameter required but not present
- **packet-too-big—**Fragmentation needed and DF set
- **parameter-problem—**All parameter problems
- **port-unreachable—**Port unreachable
- **precedence-unreachable—**Precedence cutoff
- **protocol-unreachable—**Protocol unreachable
- **reassembly-timeout—**Reassembly timeout
- **redirect—**All redirects
- **router-advertisement—**Router discovery advertisements
- **router-solicitation—**Router discovery solicitations
- **source-quench—**Source quenches
- **source-route-failed—**Source route failed
- **time-exceeded—**All time-exceeded messages
- **timestamp-reply—**Time-stamp replies
- **timestamp-request—**Time-stamp requests
- **traceroute—**Traceroute
- **ttl-exceeded—**TTL exceeded
- **unreachable—**All unreachables

TCP Port Names

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

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—EXEC (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (20)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—UNIX-to-UNIX Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 80)

UDP Port Names

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

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

non500-isakmp—Internet Security Association and Key Management Protocol (45)

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

xdmcp—X Display Manager Control Protocol (177)

Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules that deny all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network and a final rule that permits all other IPv4 traffic:

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

This example shows how to configure an IPv4 ACL named acl-eng-to-marketing with a rule that denies all IP traffic from an IPv4 address object group named eng_workstations to an IP address object group named marketing_group followed by a rule that permits all other IPv4 traffic:

```
switch# configure terminal
switch(config)# ip access-list acl-eng-to-marketing
switch(config-acl)# deny ip addrgroup eng_workstations addrgroup marketing_group
switch(config-acl)# permit ip any any
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ip access-list	Configures an IPv4 ACL.
object-group ip address	Configures an IPv4 address object group.
object-group ip port	Configures an IP port object group.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
remark	Configures a remark in an IPv4 ACL.
show ip access-list	Displays all IPv4 ACLs or one IPv4 ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
time-range	Configures a time range.

deny (IPv6)

To create an IPv6 ACL rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

General Syntax

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no deny *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*| **no**] **deny icmp** *source destination* [*icmp-message*| *icmp-type* [*icmp-code*]] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Protocol v6

[*sequence-number*] **deny ipv6** *source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Stream Control Transmission Protocol

[*sequence-number*| **no**] **deny sctp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [*flags*] **[established]** [**packet-length** *operator packet-length* [*packet-length*]]

User Datagram Protocol

[*sequence-number*| **no**] **deny udp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Syntax Description

sequence-number	(Optional) Sequence number of the deny command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.

protocol	

Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords:

- **ahp—**Specifies that the rule applies to Authentication Header Protocol (AHP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **esp—**Specifies that the rule applies to Encapsulating Security Payload (ESP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **icmp—**Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **ipv6—**Specifies that the rule applies to all IPv6 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **pcp—**Specifies that the rule applies to Payload Compression Protocol (PCP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **sctp—**Specifies that the rule applies to Stream Control Transmission Protocol (SCTP) traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **tcp—**Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **udp—**Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol*

	argument.
source	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

dscp *dscp*	

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

	• **cs7—**CS7, precedence 7 (111000) • **default—**Default DSCP value (000000) • **ef—**Expedited Forwarding (101110)
flow-label *flow-label-value*	(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575.
fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: • ACL name • Whether the packet was permitted or denied • Whether the protocol was TCP, UDP, ICMP or a number • Source and destination addresses and, if applicable, source and destination port numbers
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(ICMP only: Optional) ICMPv6 message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under "ICMPv6 Message Types" in the "Usage Guidelines" section.

icmp-type [*icmp-code*]	(ICMP only: Optional) ICMP message type that the rule matches. Valid values for the *icmp-type* argument are an integer from 0 to 255. If the ICMP message type supports message codes, you can use the *icmp-code* argument to specify the code that the rule matches. For more information about ICMP message types and codes, see http://www.iana.org/assignments/icmp-parameters .
operator port [*port*]	(Optional; TCP, UDP, and SCTP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see “TCP Port Names” and “UDP Port Names” in the “Usage Guidelines” section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the port in the packet is equal to the *port* argument. • **gt**—Matches only if the port in the packet is greater than and not equal to the *port* argument. • **lt**—Matches only if the port in the packet is less than and not equal to the *port* argument. • **neq**—Matches only if the port in the packet is not equal to the *port* argument. • **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.

portgroup *portgroup*	(Optional; TCP, UDP, and SCTP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
established	(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.
flags	(TCP only; Optional) Rule matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**

packet-length*operatorpacket-length* [*packet-length*	(Optional) Rule matches only packets that have a length in bytes that satisfies the condition specified by the *operator* and *packet-length* arguments. Valid values for the *packet-length* argument are whole numbers from 20 to 9210. The *operator* argument must be one of the following keywords: • **eq**—Matches only if the packet length in bytes is equal to the *packet-length* argument. • **gt**—Matches only if the packet length in bytes is greater than the *packet-length* argument. • **lt**—Matches only if the packet length in bytes is less than the *packet-length* argument. • **neq**—Matches only if the packet length in bytes is not equal to the *packet-length* argument. • **range**—Requires two *packet-length* arguments and matches only if the packet length in bytes is equal to or greater than the first *packet-length* argument and equal to or less than the second *packet-length* argument.

Command Default

None

Command Modes

IPv6 ACL configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

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

This command does not require a license.

Source and Destination

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

- IPv6 address group object—You can use an IPv6 address group object to specify a *source* or *destination* argument. Use the **object-group ipv6 address** command to create and change IPv6 address group objects. The syntax is as follows:

```
addrgroup

address-group-name
```

The following example shows how to use an IPv6 address object group named lab-svrs-1301 to specify the *destination* argument:

```
switch(config-acl)# deny ipv6 any addrgroup lab-svrs-1301
```

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

```
IPv6-address/prefix-len
```

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

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

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

```
host
IPv6-address
```

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

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

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

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

ICMPv6 Message Types

The *icmp-message* argument can be one of the following keywords:

- **beyond-scope**—Destination beyond scope
- **destination-unreachable**—Destination address is unreachable
- **echo-reply**—Echo reply
- **echo-request**—Echo request (ping)
- **header**—Parameter header problems
- **hop-limit**—Hop limit exceeded in transit
- **mld-query**—Multicast Listener Discovery Query
- **mld-reduction**—Multicast Listener Discovery Reduction

- **mld-report**—Multicast Listener Discovery Report
- **nd-na**—Neighbor discovery neighbor advertisements
- **nd-ns**—Neighbor discovery neighbor solicitations
- **next-header**—Parameter next header problems
- **no-admin**—Administration prohibited destination
- **no-route**—No route to destination
- **packet-too-big**—Packet too big
- **parameter-option**—Parameter option problems
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—Neighbor redirect
- **renum-command**—Router renumbering command
- **renum-result**—Router renumbering result
- **renum-seq-number**—Router renumbering sequence number reset
- **router-advertisement**—Neighbor discovery router advertisements
- **router-renumbering**—All router renumbering
- **router-solicitation**—Neighbor discovery router solicitations
- **time-exceeded**—All time exceeded messages
- **unreachable**—All unreachable

TCP Port Names

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

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—Exec (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (20)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—Unix-to-Unix Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 80)

UDP Port Names

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

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

non500-isakmp—Internet Security Association and Key Management Protocol (45)

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

xdmcp—X Display Manager Control Protocol (177)

Examples

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

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

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

```
switch# config t
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# deny ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ipv6 access-list	Configures an IPv6 ACL.
object-group ipv6 address	Configures an IPv6-address object group.
object-group ip port	Configures an IP-port object group.

Command	Description
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
remark	Configures a remark in an ACL.
show ipv6 access-list	Displays all IPv6 ACLs or one IPv6 ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
time-range	Configures a time range.

deny (MAC)

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

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*] [**time-range** *time-range-name*]

no deny *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*] [**time-range** *time-range-name*]

no *sequence-number*

Syntax Description

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

vlan *VLAN-ID*	(Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the VLAN ID given. The *VLAN-ID* argument can be an integer from 1 to 4094.
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.

Command Default

A newly created MAC ACL contains no rules.

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

Command Modes

MAC ACL configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Source and Destination

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

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

```
MAC-address MAC-mask
```

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

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

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

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

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

MAC Protocols

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

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

Examples

This example shows how to configure a MAC ACL named mac-ip-filter with rules that permit any non-IPv4 traffic between two groups of MAC addresses:

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

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
permit (MAC)	Configures a deny rule in a MAC ACL.
remark	Configures a remark in an ACL.
show mac access-list	Displays all MAC ACLs or one MAC ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
time-range	Configures a time range.

deny (role-based access control list)

To configure a deny action in the security group access control list (SGACL), use the **deny** command. To remove the action, use the **no** form of this command.

[2]**deny** {**all**| **icmp**| **igmp**| **ip**}{**tcp**| **udp**} [{**src**| **dst**}{ | {**eq** | **gt**| **lt**| **neq**}| *port -number*}| **range** {*port-number 1*| *port-number 2*}[**log**]

no deny {**all**| **icmp**| **igmp**| **ip**}{**tcp**| **udp**} [{**src**| **dst**}{ | {**eq** | **gt**| **lt**| **neq**}| *port -number*}| **range** {*port-number 1*| *port-number 2*}[**log**]

Syntax Description

all	Specifies all traffic.
icmp	Specifies Internet Control Message Protocol (ICMP) traffic.
igmp	Specifies Internet Group Management Protocol (IGMP) traffic.
ip	Specifies IP traffic.
tcp	Specifies TCP traffic.
udp	Specifies User Datagram Protocol (UDP) traffic.
src	Specifies the source port number.
dst	Specifies the destination port number.
eq	Specifies equal to the port number.
gt	Specifies greater than the port number.
lt	Specifies less than the port number.
neq	Specifies not equal to the port number.
port-number	Port number for TCP or UDP. The range is from 0 to 65535.
range	Specifies a port range for TCP or UDP.
port-number1	First port in the range. The range is from 0 to 65535.
port-number2	Last port in the range. The range is from 0 to 65535.

[2]

log	(Optional) Specifies that packets matching this configuration be logged.

Command Default

None

Command Modes

role-based access control list

Command History

Release	Modification
5.0(2)	The **log** keyword was added to support the enabling of role-based access control list (RBACL) logging.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

To enable RBACL logging, you must enable RBACL policy enforcement on the VLAN and VRF.

To enable RBACL logging, you must set the logging level of ACLLOG syslogs to 6 and the logging level of CTS manager syslogs to 5.

This command requires the Advanced Services license.

Examples

This example shows how to add a deny action to an SGACL and enable RBACL logging:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# deny icmp log
```

This example shows how to remove a deny action from an SGACL:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no deny icmp log
```

Related Commands

Command	Description
cts role-based access-list	Configures Cisco TrustSec SGACLs.
feature cts	Enables the Cisco TrustSec feature.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

description (identity policy)

To configure a description for an identity policy, use the **description** command. To revert to the default, use the **no** form of this command.

description *text*

no description

Syntax Description

"*text*"	Text string that describes the identity policy. The string is alphanumeric. The maximum length is 100 characters.

Command Default

None

Command Modes

Identity policy 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 configure the description for an identity policy:

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

This example shows how to remove the description from an identity policy:

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

Related Commands

Command	Description
identity policy	Creates or specifies an identity policy and enters identity policy configuration mode.
show identity policy	Displays identity policy information.

description (user role)

To configure a description for a user role, use the **description** command. To revert to the default, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Text string that describes the user role. The string is alphanumeric. The maximum length is 128 characters.

Command Default

None

Command Modes

User role configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can include blank spaces in the user role description text.

This command does not require a license.

Examples

This example shows how to configure the description for a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

This example shows how to remove the description from a user role:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no description
```

Related Commands

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

destination interface

To configure a destination for ACL capture packets, use the destination interface command.

destination interface ethernet *slot/port*

Syntax Description

ethernet	Specifies Ethernet IEEE 802.3z.
slot/port	Slot and port identifiers for the interface. The range is from 1 to 253.

Command Default

None

Command Modes

ACL capture configuration mode (config-acl-capture)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

Only the physical interface can be used for the destination. Port-channel interfaces and supervisor in-band ports are not supported.

Port channels and supervisor in-band ports are not supported as a destination for ACL capture.

ACL capture session destination interfaces do not support ingress forwarding and ingress MAC learning. If a destination interface is configured with these options, the monitor keeps the ACL capture session down. Use the show monitor session all command to see if ingress forwarding and MAC learning are enabled.

Note You can use the no switchport monitor command to disable ingress forwarding and MAC learning on the interface.

The source port of the packet and the ACL capture destination port cannot be part of the same ASIC. If both ports belong to the same ASIC, a message appears when you configure the destination ports for ACL capture, and the packet is not captured.

You can enter the destination interface command multiple times to add multiple destinations.

This command does not require a license.

Examples

This example shows how to configure a destination for ACL capture packets:

```
switch# configure terminal
```

```
switch(config)# monitor session 7 type acl-capture
switch(config-acl-capture)# destination interface ethernet 5/5
```

Related Commands

Command	Description
monitor session session type acl-capture	Configures an ACL capture session.

device

To add a supplicant device to the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) identity profile exception list, use the **device** command. To remove a supplicant device, use the **no** form of this command.

device {**authenticate**| **not-authenticate**} {**ip-address** *ipv4-address* [*subnet-mask*]| **mac-address** *mac-address* [*mac-address-mask*]} **policy** *policy-name*

no device {**authenticate**| **not-authenticate**} {**ip-address** *ipv4-address* [*subnet-mask*]| **mac-address** *mac-address* [*mac-address-mask*]} **policy** *policy-name*

Syntax Description

authenticate	Specifies to allow authentication of the device using the policy.
not-authenticate	Specifies to not allow authentication of the device using the policy.
ip-address *ipv4-address*	Specifies the IPv4 address for the supplicant device in the A.B.C.D format.
subnet-mask	(Optional) IPv4 subnet mask for the IPv4 address.
mac-address *mac-address*	Specifies the MAC address for the supplicant device in the XXXX.XXXX.XXXX format.
mac-address-mask	(Optional) Mask for the MAC address.
policy *policy-name*	Specifies the policy to use for the supplicant device.

Command Default

None

Command Modes

Identity policy 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 add a device to the EAPoUDP identity profile:

```
switch# configure terminal
switch(config)# identity profile eapoupd
switch(config-id-policy)# device authenticate 10.10.1.1 255.255.255.245 policy AdminPolicy
```

This example shows how to remove a device from the EAPoUDP identity profile:

```
switch# configure terminal
switch(config)# identity profile eapoupd
switch(config-id-policy)# no device authenticate 10.10.2.2 255.255.255.245 policy UserPolicy
```

Related Commands

Command	Description
identity policy	Creates or specifies an identity policy and enters identity policy configuration mode.
show identity policy	Displays identity policy information.

device-role

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping policy configuration mode or router advertisement (RA) guard policy configuration mode.

device-role {**host**| **monitor**| **router**}

Syntax Description

host	Sets the role of the device to host.
monitor	Sets the role of the device to monitor.
router	Sets the role of the device to router.

Command Default

The device role is host.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the **monitor** keyword does not allow inbound RA or redirect messages. When the **monitor** keyword is used, devices that need these messages will receive them.

Examples

The following example defines an RA guard policy name as raguard1, places the device in RA guard policy configuration mode, and configures the device as the host:

```
switch(config)# ipv6 nd raguard policy raguard1
switch(config-ra-guard)# device-role host
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

dot1x default

To reset the 802.1X global or interface configuration to the default, use the **dot1x default** command.

dot1x default

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to set the global 802.1X parameters to the default:

```
switch# configure terminal
switch(config)# dot1x default
```

This example shows how to set the interface 802.1X parameters to the default:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x default
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x	Displays 802.1X feature status information.

dot1x host-mode

To allow 802.1X authentication for either a single supplicant or multiple supplicants on an interface, use the **dot1x host-mode** command. To revert to the default, use the **no** form of this command.

dot1x host-mode {**multi-host**| **single-host**}

no dot1x host-mode

Syntax Description

mutli-host	Allows 802.1X authentication for multiple supplicants on the interface.
single-host	Allows 802.1X authentication for only a single supplicant on the interface.

Command Default

single-host

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to allow 802.1X authentication of multiple supplicants on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x host-mode multi-host
```

This example shows how to revert to the default host mode on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x host-mode
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

Command	Description
show dot1x all	Displays all 802.1X information.

dot1x initialize

To initialize 802.1X authentication for supplicants, use the **dot1x initialize** command.

dot1x initialize [**interface ethernet** *slot* | *port*]

Syntax Description

interface ethernet *slot / port*	(Optional) Specifies the interface for 802.1X authentication initialization.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to initialize 802.1X authentication for supplicants on the Cisco NX-OS device:

```
switch# dot1x initialize
```

This example shows how to initialize 802.1X authentication for supplicants on an interface:

```
switch# dot1x initialize interface ethernet 2/1
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

dot1x mac-auth-bypass

To enable MAC address authentication bypass on interfaces with no 802.1X supplicants, use the **dot1x mac-auth-bypass** command. To disable MAC address authentication bypass, use the **no** form of this command.

dot1x mac-auth-bypass [eap]

no dot1x mac-auth-bypass

Syntax Description

eap	Specifies that the bypass use Extensible Authentication Protocol (EAP).

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

This command does not require a license.

Examples

This example shows how to enable MAC address authentication bypass:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x mac-auth-bypass
```

This example shows how to disable MAC address authentication bypass:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x mac-auth-bypass
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show dot1x all	Displays all 802.1X information.

E Commands

encrypt pause-frame

To configure pause frame encryption for Cisco Trusted Security (Cisco TrustSec) on an interface, use the **encrypt pause-frame** command. To remove the pause frame encryption, use the **no** form of this command.

encrypt pause-frame

no encrypt pause-frame

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled on the line cards that support the encryption of pause frames

Command Modes

Cisco TrustSec 802.1X configuration mode (config-if-cts-manual) Cisco TrustSec manual configuration mode (config-if-cts-dotx1)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

You must enable flow control on the interface by using the flowcontrol {send | receive} command.

When you enter the no encrypt pause-frame command, the pause frames are sent as unencypted. When you enter the encrypt pause-frame command, pause frames are sent encrypted over the Cisco TrustSec link.

You cannot enable Cisco TrustSec on interfaces in half-duplex mode. Use the show interface command to determine if an interface is configured for half-duplex mode.

Note F1 Series modules, F2 Series modules, F2e Series modules, and the N7K-M132XP-12(L) module support only clear pause frames. All other M1 Series modules support both secure (encrypted and decrypted) and clear pause frames.

Caution For the pause frame encryption or decryption configuration to take effect, you must enable and disable the interface, which disrupts traffic on the interface.

This command does not require a license.

Examples

This example shows how to decrypt an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/2
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no encrypt pause-frame
switch(config-if-cts-dot1x)exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

Related Commands

Command	Description
cts dot1x	Enables Cisco TrustSec authentication on an interface and enters Cisco TrustSec 802.1X configuration mode.
cts manual	Enters Cisco TrustSec manual configuration mode for an interface.
show cts interface	Displays the Cisco TrustSec configuration information for interfaces.

encryption decrypt type6

To convert type-6 encrypted passwords back to their original state, use the encryption decrypt type6 command.

encryption decrypt type6

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to convert type6 encrypted passwords back to their original state:

```
switch # encryption decrypt type6
Please enter current Master Key:
```

Related Commands

Command	Description
encryption re-encrypt obfuscated	Converts the existing obfuscated passwords to type6 encrypted passwords.
key config-key	Configures the master key for the type-6 encryption.

encryption delete type6

To delete strongly encrypted passwords on the NX-OS device, use the encryption delete type6 command.

encryption delete type6

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to delete strongly encrypted passwords:

```
switch# configure terminal
encryption delete type6
Please enter current Master Key:
switch(config)#
```

Related Commands

Command	Description
encryption re-encrypt obfuscated	Converts the existing obfuscated passwords to type-6 encrypted passwords
key config-key	Configures the master key for the type-6 encryption.

enable

To enable a user to move to a higher privilege level after being prompted for a secret password, use the **enable** command.

enable *level*

Syntax Description

level	Privilege level to which the user must log in. The only available level is 15.

Command Default

Privilege level 15

Command Modes

EXEC configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command.

This command does not require a license.

Examples

This example shows how to enable the user to move to a higher privilege level after being prompted for a secret password:

```
switch# enable 15
```

Related Commands

Command	Description
enable secret priv-lvl	Enables a secret password for a specific privilege level.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.

Command	Description
username *user-id* priv-lvl	Enables a user to use privilege levels for authorization.

enable Cert-DN-match

To enable LDAP users to login only if the user profile lists the subject-DN of the user certificate as authorized for login, use the **enable Cert-DN-match** command. To disable this configuration, use the **no** form of this command.

enable Cert-DN-match

no enable Cert-DN-match

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

LDAP server group 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 LDAP users to login only if the user profile lists the subject-DN of the user certificate as authorized for login:

```
switch# configure terminal
switch(config)# aaa group server ldap LDAPServer1
switch(config-ldap)# server 10.10.2.2
switch(config-ldap)# enable Cert-DN-match
switch(config-ldap)
```

Related Commands

Command	Description
aaa group server ldap	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.
enable user-server-group	Enables group validation for an LDAP server group.
server	Configures the LDAP server as a member of the LDAP server group.
show ldap-server groups	Displays the LDAP server group configuration.

enable secret

To enable a secret password for a specific privilege level, use the **enable secret** command. To disable the password, use the **no** form of this command.

enable secret [**0**| **5**] **password** [**priv-lvl priv-lvl**| **all**]

no enable secret [**0**| **5**] **password** [**priv-lvl priv-lvl**| **all**]

Syntax Description

0	(Optional) Specifies that the password is in clear text.
5	(Optional) Specifies that the password is in encrypted format.
password	Password for user privilege escalation. It contains up to 64 alphanumeric, case-sensitive characters.
priv-lvl *priv-lvl*	(Optional) Specifies the privilege level to which the secret belongs. The range is from 1 to 15.
all	Adds or removes all privilege level secrets.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command.

This command does not require a license.

Examples

This example shows how to enable a secret password for a specific privilege level:

```
switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret 5 def456 priv-lvl 15
switch(config)# username user2 priv-lvl 15
switch(config)#
```

Related Commands

Command	Description
enable *level*	Enables the user to move to a higher privilege level after being prompted for a secret password.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
username *user-id* priv-lvl	Enables a user to use privilege levels for authorization.

enable user-server-group

To enable group validation for an LDAP server group, use the **enable user-server-group** command. To disable group validation, use the **no** form of this command.

enable user-server-group

no enable user-server-group

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

LDAP server group configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must configure the LDAP server group name in the LDAP server.

Users can login through public-key authentication only if the username is listed as a member of this configured group in the LDAP server.

This command does not require a license.

Examples

This example shows how to enable group validation for an LDAP server group:

```
switch# configure terminal
switch(config)# aaa group server ldap LDAPServer1
switch(config-ldap)# server 10.10.2.2
switch(config-ldap)# enable user-server-group
switch(config-ldap)
```

Related Commands

Command	Description
aaa group server ldap	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.
enable Cert-DN-match	Enables LDAP users to login only if the user profile lists the subject-DN of the user certificate as authorized for login.

Command	Description
server	Configures the LDAP server as a member of the LDAP server group.
show ldap-server groups	Displays the LDAP server group configuration.

encryption re-encrypt obfuscated

To convert the existing obfuscated passwords to type-6 encrypted passwords, use the encryption re-encrypt obfuscated command.

encryption re-encrypt obfuscated

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

When you use the encryption re-encrypt obfuscated command, the encrypted secrets such as, plain or weakly-encrypted passwords, are converted to type-6 encryption if the encryption service is enabled with a master key.

This command does not require a license.

Examples

This example shows how to convert the existing obfuscated passwords to type-6 encrypted passwords:

```
switch # encryption re-encrypt obfuscated
```

Related Commands

Command	Description
encryption decrypt type6	Converts type6 encrypted passwords back to their original state.

enrollment terminal

To enable manual cut-and-paste certificate enrollment through the switch console, use the **enrollment terminal** command. To revert to the default certificate enrollment process, use the **no** form of this command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Command Default

The default is the manual cut-and-paste method, which is the only enrollment method that the Cisco NX-OS software supports.

Command Modes

Trustpoint 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 trustpoint enrollment through the switch console:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# enrollment terminal
```

This example shows how to discard a trustpoint enrollment through the switch console:

```
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# no
 enrollment terminal
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the certificate authority.

eou allow clientless

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) posture validation of clientless endpoint devices, use the **eou allow clientless** command. To disable posture validation of clientless endpoint devices, use the **no** form of this command.

eou allow clientless

no eou allow clientless

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to allow EAPoUDP posture validation of clientless endpoint devices:

```
switch# config t
switch(config)# eou allow clientless
```

This example shows how to prevent EAPoUDP posture validation of clientless endpoint devices:

```
switch# config t
switch(config)# no eou allow clientless
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

eou default

To revert to the default global or interface configuration values for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou default** command.

eou default

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the global EAPoUDP configuration to the default:

```
switch# config t
switch(config)# eou default
```

This example shows how to change the EAPoUDP configuration for an interface to the default:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou default
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

eou initialize

To initialize Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions, use the **eou initialize** command.

eou initialize {**all**| **authentication** {**clientless**| **eap**| **static**}| **interface ethernet slot** / **port**| **ip-address ipv4-address**| **mac-address mac-address**| **posturetoken name**}

Syntax Description

all	Initializes all EAPoUDP sessions.
authentication	Initializes EAPoUDP sessions for a specific authentication types.
clientless	Specifies sessions authenticated using clientless posture validation.
eap	Specifies sessions authenticated using EAPoUDP.
static	Specifies sessions authenticated using statically configured exception lists.
interface ethernet *slot*/*port*	Initializes the EAPoUDP sessions for a specific interface.
ip-address *ipv4-address*	Initializes the EAPoUDP sessions for a specific IPv4 address.
mac-address *mac-address*	Initializes the EAPoUDP sessions for a specific MAC address.
posturetoken *name*	Initializes the EAPoUDP sessions for a specific posture token.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to initialize all the EAPoUDP sessions:

```
switch# eou initialize all
```

This example shows how to initialize the EAPoUDP sessions that were statically authenticated:

```
switch# eou initialize authentication static
```

This example shows how to initialize the EAPoUDP sessions for an interface:

```
switch# eou initialize interface ethernet 1/1
```

This example shows how to initialize the EAPoUDP sessions for an IP address:

```
switch# eou initialize ip-address 10.10.1.1
```

This example shows how to initialize all the EAPoUDP sessions for a MAC address:

```
switch# eou initialize mac-address 0019.076c.dac4
```

This example shows how to initialize all the EAPoUDP sessions for a posture token:

```
switch# eou initialize posturetoken healthy
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

eou logging

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) logging, use the **eou logging** command. To disable EAPoUDP logging, use the **no** form of this command.

eou logging

no eou logging

Syntax Description

This command has no arguments or keywords.

Command Default

Global configuration: Disabled

Interface configuration: Global configuration setting

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The setting for EAPoUDP logging on an interface overrides the global setting.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to enable global EAPoUDP logging:

```
switch# config t
switch(config)# eou logging
```

This example shows how to disable global EAPoUDP logging:

```
switch# config t
switch(config)# no eou logging
```

This example shows how to enable EAPoUDP logging for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou logging
```

This example shows how to disable EAPoUDP logging for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no eou logging
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

eou max-retry

To configure the maximum number of attempts for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) globally or for an interface, use the **eou max-retry** command. To revert to the default, use the **no** form of this command.

eou max-retry *count*

no eou max-retry

Syntax Description

count	Maximum number of retry attempts. The range is from 1 to 3.

Command Default

Global configuration: 3

Interface configuration: global configuration value

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The maximum retries for an interface takes precedence over the globally configured value.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the global maximum number of EAPoUDP retry attempts:

```
switch# config t
switch(config)# eou max-retry 2
```

This example shows how to revert to the default global maximum number of EAPoUDP retry attempts:

```
switch# config t
switch(config)# no eou max-retry
```

This example shows how to change the maximum number of EAPoUDP retry attempts for an interface:

```
switch# config t
switch(config) interface ethernet 1/1
switch(config-if)# eou max-retry 3
```

This example shows how to revert to the maximum number of EAPoUDP retry attempts for an interface:

```
switch# config t
switch(config) interface ethernet 1/1
switch(config-if)# no eou max-retry
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

eou port

To configure the User Datagram Protocol (UDP) port number for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou port** command. To revert to the default, use the **no** form of this command.

eou port *udp-port*

no eou port

Syntax Description

udp-port	UDP port number. The range is from 1 to 65535.

Command Default

21862 (0x5566)

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the UDP port number for EAPoUDP:

```
switch# config t
switch(config)# eou port 21856
```

This example shows how to revert to the default UDP port number for EAPoUDP:

```
switch# config t
switch(config)# no eou port
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

eou ratelimit

To configure the number of simultaneous posture validation sessions for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou ratelimit** command. To revert to the default, use the **no** form of this command.

eou ratelimit *sessions*

no eou ratelimit

Syntax Description

sessions	Maximum number of simultaneous EAPoUDP posture validation sessions. The range is from 0 to 200.

Command Default

Global configuration: 20

Interface configuration: Global configuration setting

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Setting the EAPoUDP rate limit to zero (0) allows no simultaneous posture validation sessions.

The EAPoUDP rate limit for an interface overrides the globally EAPoUDP rate limit setting.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the global maximum number of simultaneous EAPoUDP posture-validation sessions:

```
switch# config t
switch(config)# eou ratelimit 30
```

This example shows how to revert to the default global maximum number of simultaneous EAPoUDP posture-validation sessions:

```
switch# config t
switch(config)# no eou ratelimit
```

This example shows how to change the maximum number of simultaneous EAPoUDP posture-validation sessions for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou ratelimit 30
```

This example shows how to revert to the default maximum number of simultaneous EAPoUDP posture-validation sessions for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no eou ratelimit
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

eou revalidate (EXEC)

To revalidate Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions, use the **eou revalidate** command.

eou revalidate {**all**| **authentication** {**clientless**| **eap**| **static**}| **interface ethernet slot** / **port**| **ip-address ipv4-address**| **mac-address mac-address**| **posturetoken name**}

Syntax Description

all	Revalidates all EAPoUDP sessions.
authentication	Revalidates EAPoUDP sessions for specific authentication types.
clientless	Specifies sessions authenticated using clientless posture validation.
eap	Specifies sessions authenticated using EAPoUDP.
static	Specifies sessions authenticated using statically configured exception lists.
interface ethernet *slot/port*	Revalidates the EAPoUDP sessions for a specific interface.
ip-address *ipv4-address*	Revalidates the EAPoUDP sessions for a specific IPv4 address.
mac-address *mac-address*	Revalidates the EAPoUDP sessions for a specific MAC address.
posturetoken *name*	Revalidates the EAPoUDP sessions for a specific posture token.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Note The Cisco NX-OS software supports an **eou revalidate** command in global configuration mode. To use an EXEC-level **eou revalidate** command in global configuration mode, include the required keywords.

Examples

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate all
```

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate authentication static
```

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate interface ethernet 1/1
```

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate ip-address 10.10.1.1
```

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate mac-address 0019.076c.dac4
```

This example shows how to revalidate all the EAPoUDP sessions:

```
switch# eou revalidate posturetoken healthy
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

eourevalidate(globalconfigurationandinterfaceconfiguration)

To enable automatic periodic revalidation of Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions globally or for a specific interface, use the **eou revalidate** command. To revert to the default, use the **no** form of this command.

eou revalidate

no eou revalidate

Syntax Description

This command has no arguments or keywords.

Command Default

Global configuration: Enabled

Interface configuration: Global configuration value

Command Modes

Global configuration Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The automatic revalidation setting for an interface overrides the global setting for automatic revalidation.

Note The Cisco NX-OS software supports an **eou revalidate** command in EXEC configuration mode. To use an EXEC-level **eou revalidate** command in global configuration mode, include the required keywords.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to disable global automatic revalidation of EAPoUDP sessions:

```
switch# config t
switch(config)# no eou revalidate
```

This example shows how to enable global automatic revalidation of EAPoUDP sessions:

```
switch# config t
switch(config)# eou revalidate
```

This example shows how to disable automatic revalidation of EAPoUDP sessions for an interface:

```
switch# config t
switch(config)# no eou revalidate
```

This example shows how to enable automatic revalidation of EAPoUDP sessions for an interface:

```
switch# config t
switch(config)# eou revalidate
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
eou timeout	Configures the timeout interval for EAPoUDP automatic periodic validation.
show eou	Displays EAPoUDP information.

eou timeout

To configure timeout intervals for the global Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) timers or for the EAPoUDP timers for an interface, use the **eou timeout** command. To revert to the default, use the **no** form of this command.

eou timeout {**aaa** *seconds*| **hold-period** *seconds*| **retransmit** *seconds*| **revalidation** *seconds*| **status-query** *seconds*}

no eou timeout {**aaa**| **hold-period**| **retransmit**| **revalidation**| **status-query**}

Syntax Description

aaa *seconds*	Specifies the AAA timeout interval. The range is from 0 to 60 seconds. **Note** Setting the AAA timeout interval to zero (0) disables the AAA timer.
hold-period *seconds*	Specifies the hold timeout interval. The range is from 60 to 86400 seconds.
retransmit *seconds*	Specifies the retransmit timeout interval. The range is from 1 to 60 seconds.
revalidation *seconds*	Specifies the period automatic revalidation timeout interval. The range is from 5 to 86400 seconds.
status-query *seconds*	Specifies the status query timeout interval. The range is from 10 to 1800 seconds.

Command Default

Global AAA timeout interval: 60 seconds (1 minute)

Global hold-period timeout: 180 seconds (3 minutes)

Global retransmit timeout interval: 3 seconds

Global revalidation timeout interval: 36000 seconds (10 hours)

Global status query timeout interval: 300 seconds (5 minutes)

Interface timeout intervals: Global configuration values

Command Modes

Global configurationInterface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The timeout interval values for the interface timers override the global timeout values.

You must use the **feature eou** command before you configure EAPoUDP.

This command does not require a license.

Examples

This example shows how to change the global AAA timeout interval:

```
switch# config t
switch(config)# eou timeout aaa 50
```

This example shows how to change the AAA timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout aaa 60
```

This example shows how to change the global hold-period timeout interval:

```
switch# config t
switch(config)# eou timeout hold-period 480
```

This example shows how to change the hold-period timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout hold-period 540
```

This example shows how to change the global retransmit timeout interval:

```
switch# config t
switch(config)# eou timeout retransmit 5
```

This example shows how to change the retransmit timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout retransmit 4
```

This example shows how to change the global revalidation timeout interval:

```
switch# config t
switch(config)# eou timeout revalidation 34000
```

This example shows how to change the revalidation timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout revalidation 30000
```

This example shows how to change the global status-query timeout interval:

```
switch# config t
switch(config)# eou timeout status-query 240
```

This example shows how to change the status-query timeout interval for an interface:

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout status-query 270
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
eou revalidate (global configuration)	Enables periodic automatic revalidation of endpoint devices.
show eou	Displays EAPoUDP information.

eq

To specify a single port as a group member in an IP port object group, use the **eq** command. To remove a single port group member from the port object group, use the **no** form of this command.

[*sequence-number*] **eq** *port-number*

no {*sequence-number*| **eq** *port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
port-number	Port number that this group member matches. Valid port numbers are from 0 to 65535.

Command Default

None

Command Modes

IP port object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether an **eq** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 443:

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# eq 443
```

Related Commands

Command	Description
gt	Specifies a greater-than group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.
object-group ip port	Configures an IP port object group.
range	Specifies a port-range group member in an IP port object group.
show object-group	Displays object groups.

F Commands

feature (user role feature group)

To configure a feature in a user role feature group, use the **feature** command. To delete a feature in a user role feature group, use the **no** form of this command.

feature *feature-name*

no feature *feature-name*

Syntax Description

feature-name	Cisco NX-OS feature name as listed in the **show role feature** command output.

Command Default

None

Command Modes

User role feature group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the show role feature command to list the valid feature names to use in this command.

This command does not require a license.

Examples

This example shows add features to a user role feature group:

```
switch# configure terminal
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

This example shows how to remove a feature from user role feature group:

```
switch# configure terminal
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)# no feature callhome
```

Related Commands

Command	Description
show role feature-group	Displays the user role feature groups.

feature cts

To enable the Cisco TrustSec feature, use the **feature cts** command. To revert to the default, use the **no** form of this command.

feature cts

no feature cts

Syntax Description

This command has no arguments or keywords.

Command Default

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 Cisco TrustSec feature using the **feature dot1x** command.

The users can enable feature cts command even without having any license installed.

Note The Cisco TrustSec feature does not have a license grace period. You must install the Advanced Services license to configure this feature.

This command requires the Advanced Services license.

Examples

This example shows how to enable the Cisco TrustSec feature:

```
switch# configure terminal
switch(config)# feature cts
```

This example shows how to disable the Cisco TrustSec feature:

```
switch# configure terminal
switch(config)# no feature cts
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.
show cts	Displays the Cisco TrustSec status information.

feature dhcp

To enable the DHCP snooping feature on the device, use the **feature dhcp** command. To disable the DHCP snooping feature and remove all configuration related to DHCP snooping, including DHCP relay, dynamic ARP inspection (DAI), and IP Source Guard configuration, use the **no** form of this command.

feature dhcp

no feature dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The DHCP snooping feature is disabled by default.

If you have not enabled the DHCP snooping feature, commands related to DCHP snooping are unavailable.

Dynamic ARP inspection and IP Source Guard depend upon the DHCP snooping feature.

If you disable the DHCP snooping feature, the device discards all configuration related to DHCP snooping configuration, including the following features:

- DHCP snooping
- DHCP relay
- DAI
- IP Source Guard

If you want to turn off DHCP snooping and preserve configuration related to DHCP snooping, disable DHCP snooping globally with the **no ip dhcp snooping** command.

Access-control list (ACL) statistics are not supported if the DHCP snooping feature is enabled.

This command does not require a license.

Examples

This example shows how to enable DHCP snooping:

```
switch# configure terminal
```

```
switch(config)# feature dhcp
switch(config)#'
```

Related Commands

Command	Description
clear ip dhcp snooping binding	Clears the DHCP snooping binding database.
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.

feature dot1x

To enable the 802.1X feature, use the **feature dot1x** command. To revert to the default, use the **no** form of this command.

feature dot1x

no feature dot1x

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature dot1x** command before you configure 802.1X.

Note If you disable the 802.1X feature, all 802.1X configuration is lost. If you want to disable 802.1X authentication, use the **no dot1x system-auth-control** command.

This command does not require a license.

Examples

This example shows how to enable 802.1X:

```
switch# configure terminal
switch(config)# feature dot1x
```

This example shows how to disable 802.1X:

```
switch# configure terminal
switch(config)# no feature dot1x
```

Related Commands

Command	Description
show dot1x	Displays 802.1X status information.

feature eou

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **feature eou** command. To disable EAPoUDP, use the **no** form of this command.

feature eou

no feature eou

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command before you configure EAPoUDP.

Note When you disable EAPoUDP, the Cisco NX-OS software removes the EAPoUDP configuration.

This command does not require a license.

Examples

This example shows how to enable EAPoUDP:

```
switch# configure terminal
switch(config)# feature eou
```

This example shows how to disable EAPoUDP:

```
switch# configure terminal
switch(config)# no feature eou
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

feature ldap

To enable Lightweight Directory Access Protocol (LDAP), use the **feature ldap** command. To disable LDAP, use the **no** form of this command.

feature ldap

no feature ldap

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you configure LDAP.

Note When you disable LDAP, the Cisco NX-OS software removes the LDAP configuration.

This command does not require a license.

Examples

This example shows how to enable LDAP:

```
switch# configure terminal
switch(config)# feature ldap
```

This example shows how to disable LDAP:

```
switch# configure terminal
switch(config)# no feature ldap
```

Related Commands

Command	Description
show running-config ldap	Displays the LDAP configuration in the running configuration.
show startup-config ldap	Displays the LDAP configuration in the startup configuration.

feature mka

To enable the MACsec Key Agreement (MKA) feature, use the **feature mka** command. To disable the MKA feature, use the **no** form of this command.

feature mka

no feature mka

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
8.2(1)	This command was introduced.

Examples

This example shows how to enable the MKA feature:

```
switch# configure terminal
switch(config)# feature mka
```

This example shows how to disable the MKA feature:

```
switch# configure terminal
switch(config)# no feature mka
```

Related Commands

Command	Description
cipher suite	Configures the cipher suite for encrypting traffic with MACsec.
conf-offset	Configures the confidentiality offset for MKA encryption.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
key-octet-string	Configures the text for a MACsec key.

Command	Description
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
sak-expiry-time *time*	Sets an expiry time for a force SAK rekey.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

feature password encryption aes

To enable the Advanced Encryption Standard (AES) password encryption feature, use the **feature password encryption aes** command. To disable the AES password encryption feature, use the **no** form of this command.

feature password encryption aes

no feature password encryption aes

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode (config)

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

You can enable the AES password encryption feature without a master key, but encryption starts only when a master key is present in the system. To configure a master key, use the key config-key command.

This command does not require a license.

Examples

This example shows how to enable the AES password encryption feature:

```
switch# configure terminal
switch(config)# feature password encryption aes
switch(config)#
```

This example shows how to disable the AES password encryption feature:

```
switch(config)# no feature password encryption aes
switch(config)#
```

Related Commands

Command	Description
key config-key	Configures the master key for type-6 encryption.
show encryption service stat	Displays the status of the encryption service.

feature port-security

To enable the port security feature globally, use the **feature port-security** command. To disable the port security feature globally, use the **no** form of this command.

feature port-security

no feature port-security

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Port security is disabled globally by default.

Port security is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

This command does not require a license.

Enabling Port Security

If you enable port security globally, all other commands related to port security become available.

If you are reenabling port security, no port security configuration is restored from the last time that port security was enabled.

Disabling Port Security

If you disable port security globally, all port security configuration is removed, including any interface configuration for port security and all secured MAC addresses, regardless of the method by which the device learned the addresses.

Examples

This example shows how to enable port security globally:

```
switch# configure terminal
switch(config)# feature port-security
switch(config)#
```

Related Commands

Command	Description
clear port-security	Clears dynamically learned, secure MAC addresses.
debug port-security	Provides debugging information for port security.
show port-security	Shows information about port security.
switchport port-security	Enables port security on a Layer 2 interface.

feature privilege

To enable the cumulative privilege of roles for command authorization on TACACS+ servers, use the **feature privilege**command. To disable the cumulative privilege of roles, use the **no** form of this command.

feature privilege

no feature privilege

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

When the **feature privilege** command is enabled, privilege roles inherit the permissions of lower level privilege roles.

Examples

This example shows how to enable the cumulative privilege of roles:

```
switch# configure terminal
switch(config)# feature privilege
```

This example shows how to disable the cumulative privilege of roles:

```
switch# configure terminal
switch(config)# no feature privilege

2010 Feb 12 12:52:06 switch %FEATURE-MGR-2-FM_AUTOCKPT_IN_PROGRESS: AutoCheckpoint
system-fm-privilege's creation in progress...
switch(config)# 2010 Feb 12 12:52:06 switch %FEATURE-MGR-2-FM_AUTOCKPT_SUCCEEDED
AutoCheckpoint created successfully
```

Related Commands

Command	Description
enable *level*	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.

Command	Description
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
username *username* **priv-lvl**	Enables a user to use privilege levels for authorization.

feature scp-server

To configure a secure copy (SCP) server on the Cisco NX-OS device in order to copy files to and from a remote device, use the **feature scp-server** command. To disable an SCP server, use the **no** form of this command.

feature scp-server

no feature scp-server

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

After you enable the SCP server, you can execute an SCP command on the remote device to copy the files to or from the Cisco NX-OS device.

The arcfour and blowfish cipher options are not supported for the SCP server.

This command does not require a license.

Examples

This example shows how to enable the SCP server on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# feature scp-server
switch(config)#
```

This example shows how to disable the SCP server on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# no feature scp-server
switch(config)#
```

Related Commands

Command	Description
feature sftp-server	Enables the SFTP server on the Cisco NX-OS device.

feature sftp-server

To configure a secure FTP (SFTP) server on the Cisco NX-OS device in order to copy files to and from a remote device, use the **feature sftp-server** command. To disable an SFTP server, use the no form of this command.

feature sftp-server

no feature sftp-server

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

After you enable the SFTP server, you can execute an SFTP command on the remote device to copy the files to or from the Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enable the SFTP server on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# feature sftp-server
switch(config)#
```

This example shows how to disable the SFTP server on the Cisco NX-OS device:

```
switch# configure terminal
switch(config)# no feature sftp-server
switch(config)#
```

Related Commands

Command	Description
feature scp-server	Enables the SCP server on the Cisco NX-OS device.

feature ssh

To enable the Secure Shell (SSH) server for a virtual device context (VDC), use the **feature ssh** command. To disable the SSH server, use the **no** form of this command.

feature ssh

no feature ssh

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced to replace the **ssh server enable** command.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

This command does not require a license.

Examples

This example shows how to enable the SSH server:

```
switch# configure terminal
switch(config)# feature ssh
```

This example shows how to disable the SSH server:

```
switch# configure terminal
switch(config)# no feature ssh

XML interface to system may become unavailable since ssh is disabled
```

Related Commands

Command	Description
show feature	Displays the enable status of the features.
show ssh server	Displays the SSH server key information.

feature tacacs+

To enable TACACS+, use the **feature tacacs+** command. To disable TACACS+, use the **no** form of this command.

feature tacacs+

no feature tacacs+

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

Note When you disable TACACS+, the Cisco NX-OS software removes the TACACS+ configuration.

This command does not require a license.

Examples

This example shows how to enable TACACS+:

```
switch# configure terminal
switch(config)# feature tacacs+
```

This example shows how to disable TACACS+:

```
switch# configure terminal
switch(config)# no feature tacacs+
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ information.

feature telnet

To enable the Telnet server for a virtual device context (VDC), use the **feature telnet** command. To disable the Telnet server, use the **no** form of this command.

feature telnet

no feature telnet

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced to replace the **telnet server enable** command.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the Telnet server:

```
switch# configure terminal
switch(config)# feature telnet
```

This example shows how to disable the Telnet server:

```
switch# configure terminal
switch(config)# no feature telnet

XML interface to system may become unavailable since ssh is disabled
```

Related Commands

Command	Description
show feature	Displays the enable status of the features.
show telnet server	Displays the SSH server key information.

filter

To configure one or more certificate mapping filters within the filter map, use the **filter** command.

filter [**subject-name** *subject-name*| **altname-email** *e-mail-ID*| **altname-upn** *user-principal-name*]

Syntax Description

subject-name	(Optional) Specifies the subject name of the certificate.
subject-name	Required subject name in LDAP distinguished name (DN) string format. For example: cn=%username%,ou=PKI,o=Acme,c=US
altname-email	(Optional) Specifies the e-mail ID as an alternate name.
e-mail-ID	E-mail address that must be present in the certificate as a subject alternative name. For example: %username%@*
altname-upn	(Optional) Specifies the user principal name as an alternate name.
user-principal-name	Principal name that must be present in the certificate as a subject alternative name. For example: %username-without-domain%@%hostname%

Command Default

None

Command Modes

Certificate mapping filter configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must create a new filter map.

The validation passes if the certificate passes all of the filters configured in the map.

This command does not require a license.

Examples

This example shows how to configure a certificate mapping filter within the filter map:

```
switch# configure terminal
switch(config)# crypto certificatemap mapname filtermap1
switch(config-certmap-filter)# filter altname-email jsmith@acme.com
```

Related Commands

Command	Description
crypto certificatemap mapname	Creates a filter map.
show crypto certificatemap	Displays the certificate mapping filters.

fips mode enable

To enable Federal Information Processing Standards (FIPS) mode, use the **fips mode enable** command. To disable FIPS mode, use the no form of this command.

fips mode enable

no fips mode enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

Before enabling FIPS mode, ensure that you are in the default virtual device context (VDC).

FIPS has the following prerequisites:

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Delete all SSH server RSA1 key-pairs.
- Enable HMAC-SHA1 message integrity checking (MIC) for use during the Cisco TrustSec Security Association Protocol (SAP) negotiation. To do so, enter the sap hash-algorithm HMAC-SHA-1 command from the cts-manual or cts-dot1x mode.

This command does not require a license.

Examples

This example shows how to enable FIPS mode:

```
switch# configure terminal
switch(config)# fips mode enable

FIPS mode is enabled
```

This example shows how to disable FIPS mode:

```
switch# configure terminal
switch(config)# no fips mode enable
```

```
FIPS mode is disabled
```

Related Commands

Command	Description
show fips status	Displays the status of Federal Information Processing Standard (FIPS) mode.

fragments

To optimize whether an IPv4 or IPv6 ACL permits or denies noninitial fragments that do not match an explicit **permit** or **deny** command in the ACL, use the **fragments** command. To disable fragment optimization, use the **no** form of this command.

fragments {**deny-all**| **permit-all**}

no fragments {**deny-all**| **permit-all**}

Syntax Description

deny-all	Specifies that noninitial fragments of flows that are matched by the ACL are always dropped.
permit-all	Specifies that any noninitial fragments of a flow are permitted when the initial fragment of the flow was permitted by the ACL.

Command Default

None

Command Modes

IPv4 ACL configuration

IPv6 ACL configuration

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

The **fragments** command allows you to simplify the configuration of an IP ACL when you want to permit or deny noninitial fragments that do not match an explicit **permit** or **deny** command in the ACL. Instead of controlling noninitial fragment handling by using many **permit** or **deny** commands that specify the **fragments** keyword, you can use the **fragments** command instead.

When a device applies to traffic an ACL that contains the **fragments** command, it only matches noninitial fragments that do not match any explicit **permit** or **deny** commands in the ACL.

This command does not require a license.

Examples

This example shows how to enable fragment optimization in an IPv4 ACL named lab-acl. The **permit-all** keyword means that the ACL permits any noninitial fragment that does not match a **deny** command that includes the **fragments** keyword.

```
switch# configure terminal
```

```
switch(config)# ip access-list lab-acl
switch(config-acl)# fragments permit-all
```

This example shows the lab-acl IPv4 ACL, which includes the **fragments** command. The **fragments** command appears at the beginning of the ACL for convenience, but the device permits noninitial fragments only after they do not match all other explicit rules in the ACL.

```
switch(config-acl)# show ip access-lists lab-acl

IP access list lab-acl
fragments permit-all
10 permit tcp 10.0.0.0/8 172.28.254.254/24 eq tacacs
20 permit tcp 10.0.0.0/8 172.28.254.154/24 eq tacacs
30 permit tcp 10.0.0.0/8 172.28.254.54/24 eq tacacs
```

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
permit (IPv4)	Configures a permit rule in an IPv4 ACL.
permit (IPv6)	Configures a permit rule in an IPv6 ACL.
show ip access-list	Displays all IPv4 ACLs or a specific IPv4 ACL.
show ipv6 access-list	Displays all IPv6 ACLs or a specific IPv6 ACL.

G Commands

gt

To specify a greater-than group member for an IP port object group, use the **gt** command. A greater-than group member matches port numbers that are greater than (and not equal to) the port number specified in the member. To remove a greater-than group member from the port-object group, use the **no** form of this command.

[*sequence-number*] **gt** *port-number*

no {*sequence-number*| **gt** *port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
port-number	Port number that traffic matching this group member exceeds. The *port-number* argument can be a whole number between 0 and 65535.

Command Default

None

Command Modes

IP port object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether a **gt** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 49152 through port 65535:

```
switch# configure terminal
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# gt 49151
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.
object-group ip port	Configures an IP port object group.
range	Specifies a port-range group member in an IP port object group.
show object-group	Displays object groups.

H Commands

hardware access-list allow deny ace

To enable deny ace support for seq based feature, use the **hardware access-list allow deny ace** command. To disable this feature, use the n**no** form of the command.

hardware access-list allow deny ace

no hardware access-list allow deny ace

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
6.1(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Note Deny ace feature is not supported on F1 module.

This example shows how to enable deny ace feature:

```
switch# configure terminal
switch(config)# hardware access-list allow deny ace
switch(config)#
```

This example shows how to disable deny ace feature:

```
switch# configure terminal
switch(config)# no hardware access-list allow deny ace
switch(config)#
```

Related Commands

Command	Description
hardware access-list update	Configures how a supervisor module updates an I/O module with changes to an ACL.

hardware access-list capture

To enable access control list (ACL) capture on all virtual device contexts (VDCs), use the **hardware access-list capture** command. To disable ACL capture, use the **no** form of the command.

hardware access-list capture

no hardware access-list capture

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
6.1(1)	Added support for M2 series modules.
5.2(1)	This command was introduced.

Usage Guidelines

Only M Series modules support ACL capture.

ACL capture is a -assisted feature and is not supported for the management interface or for control packets originating in the supervisor. It is also not supported for software ACLs such as SNMP community ACLs and virtual teletype (VTY) ACLs.

Enabling ACL capture disables ACL logging for all VDCs and the rate limiter for ACL logging.

Only one ACL capture session can be active at any given time in the system across VDCs.

This command does not require a license.

Examples

This example shows how to enable ACL capture on all VDCs:

```
switch# configure terminal
switch(config)# hardware access-list capture
```

This example shows how to disable ACL capture on all VDCs:

```
switch # configure terminal
switch(config)# no hardware access-list capture
```

Related Commands

Command	Description
hardware access-list update	Configures how a supervisor module updates an I/O module with changes to an ACL.

hardware access-list resource feature bank-mapping

To enable access control list (ACL) ternary control address memory (TCAM) bank mapping for feature groups and classes, use the **hardware access-list resource feature bank-mapping** command. To disable ACL TCAM bank mapping, use the **no** form of the command.

hardware access-list resource feature bank-mapping

no hardware access-list resource feature bank-mapping

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command is available only in the default virtual device context (VDC) but applies to all VDCs.

F1 Series modules do not support ACL TCAM bank mapping. Resource pooling and ACL TCAM bank mapping cannot be enabled at the same time.

Examples

This example shows how to enable ACL TCAM bank mapping for feature groups and classes:

```
switch(config)# hardware access-list resource feature bank-mapping
```

Related Commands

Command	Description
show system internal access-list feature bank-class map	Displays the ACL TCAM bank mapping feature group and class combination tables.

hardware access-list resource pooling

To allow ACL-based features to use more than one TCAM bank on one or more I/O modules, use the **hardware access-list resource pooling** command. You can also enable flexible TCAM bank chaining feature with PORT-VLAN or VLAN-VLAN modes. To restrict ACL-based features to using one TCAM bank on an I/O module, use the **no** form of this command.

hardware access-list resource pooling [**port-vlan**| **vlan-vlan**] **module** {*module-number*| **all**}

no hardware access-list resource pooling [**port-vlan**| **vlan-vlan**] **module** {*module-number*| **all**}

Syntax Description

module	Specifies the module.
port-vlan	Specifies the port-vlan mode that allows you to configure a single port feature and a single VLAN feature on a destination per direction.
vlan-vlan	Specifies the vlan-vlan mode that allows you to configure two VLAN features on a destination per direction.
module-number	Specifies the I/O module(s). The *slot-number-list* argument allows you to specify modules by the slot number that they occupy. You can specify a single I/O module, a range of slot numbers, or comma-separated slot numbers and ranges.
all	Specifies all the modules. Note that the PORT-VLAN and VLAN-VLAN modes are supported only on the F3 modules. So, you cannot enable the flexible TCAM bank chaining for all the modules.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
7.3(0)D1(1)	This command was modified to support flexible bank chaining feature with VLAN-VLAN and PORT-VLAN modes.
4.2(1)	The hyphen was removed between the **resource** and **pooling** keywords.
4.1(2)	This command was introduced.

Usage Guidelines

By default, each ACL-based feature can use one TCAM bank on an I/O module. This default behavior limits each feature to 16,000 TCAM entries. If you have very large security ACLs, you may encounter this limit. The command allows you to make more than 16,000 TCAM entries available to ACL-based features.

If you want to enable bank chaining for the entire system, Cisco recommends adding the configuration for the entire module range, even if a module is not present, using the module range command, as described in the Examples section.

This command does not require a license.

Examples

This example shows how to enable ACL programming across TCAM banks on the I/O module in slot 1:

```
switch# configure terminal
switch(config)# hardware access-list resource pooling module 1
```

This example shows how to enable bank chaining for all modules in a 10-slot chassis (excluding supervisor slots 5 and 6):

```
switch# configure terminal
switch(config)# hardware access-list resource pooling module 1-4, 7-10
```

When a new module is inserted, bank chaining is enabled automatically for that module, without you having to remember to enter the command.

This example shows how to enable VLAN-VLAN mode for the module 3:

```
switch# configure terminal
switch(config)# hardware access-list resource pooling vlan-vlan module 3
```

Related Commands

Command	Description
hardware access-list update	Configures atomic or non-atomic update of access-list, and default access-list result during the non-atomic hardware update.
show running-config all	Displays the running configuration, including the default configuration.
show system internal access-list globals	Displays the access control list (ACL) ternary content addressable memory (TCAM) common information along with the bank chaining mode.

hardware access-list update

To configure how a supervisor module updates an I/O module with changes to an access-control list (ACL), use the **hardware access-list update** command in the default virtual device context (VDC). To disable atomic updates, use the **no** form of this command.

hardware access-list update {**atomic**| **default-result permit**}

no hardware access-list update {**atomic**| **default-result permit**}

Syntax Description

atomic	Specifies that the device performs atomic updates, which do not disrupt traffic during the update. By default, a Cisco Nexus 7000 Series device performs atomic ACL updates.
default-result permit	Specifies that, during non-atomic updates, the device permits traffic that the updated ACL applies to.

Command Default

atomic

Command Modes

Global configuration

Command History

Release	Modification
4.1(4)	This command is available only in the default VDC.
4.1(2)	This command was introduced to replace the **platform access-list update** command.

Usage Guidelines

In Cisco NX-OS Release 4.1(4) and later releases, the hardware **access-list update** command is available in the default VDC only and affects all VDCs.

By default, when a supervisor module of a Cisco Nexus 7000 Series device updates an I/O module with changes to an ACL, it performs an atomic ACL update. An atomic update does not disrupt traffic that the updated ACL applies to; however, an atomic update requires that an I/O module that receives an ACL update has enough available resources to store each updated ACL entry in addition to all preexisting entries in the affected ACL. After the update occurs, the additional resources used for the update are freed. If the I/O module lacks the required resources, the device generates an error message and the ACL update to the I/O module fails.

If an I/O module lacks the resources required for an atomic update, you can disable atomic updates by using the **no hardware access-list update atomic** command in the default VDC; however, during the brief time required for the device to remove the preexisting ACL and implement the updated ACL, traffic that the ACL applies to is dropped by default.

If you want to permit all traffic that an ACL applies to while it receives a nonatomic update, use the **hardware access-list update default-result permit** command in the default VDC.

This command does not require a license.

Examples

Note In Cisco NX-OS Release 4.1(4) and later releases, the **hardware access-list update** command is available in the default VDC only. To verify that the current VDC is the VDC 1 (the default VDC), use the **show vdc current-vdc** command.

This example shows how to disable atomic ACL updates:

```
switch# configure terminal
switch(config)# no hardware access-list update atomic
```

This example shows how to permit affected traffic during a nonatomic ACL update:

```
switch# configure terminal
switch(config)# hardware access-list update default-result permit
```

This example shows how to revert to the atomic update method:

```
switch# configure terminal
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

Related Commands

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

hardware rate-limiter

To configure rate limits in packets per second on supervisor-bound traffic, use the **hardware rate-limiter** command. To revert to the default, use the **no** form of this command.

hardware rate-limiter {**access-list-log** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **copy** {*packets*| **disable**} [**module module***module* [**port** *start end*]]| **f1** {**rl-1** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **rl-2** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **rl-3** {*packets*| **disable**} [**module** *module*[**port** *start end*]]| **rl-4** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **rl-5** {*packets*| **disable**} [**module** *module* [**port** *start end*]]}| **layer-2** {**l2pt** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **mcast-snooping** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **port-security** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **storm-control** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **vpc-low** {*packets*| **disable**} [**module** *module* [**port** *start end*]]}| **layer-3** {**control** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **glean** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **glean-fast** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **mtu** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **multicast** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **ttl** {*packets*| **disable**} [**module** *module* [**port** *start end*]]}| **receive** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| || [**portgroup-multiplier** *multiplier* **module** *module*]}

nohardware rate-limiter {**access-list-log** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **copy** {*packets*| **disable**} [**module module***module* [**port** *start end*]]| **f1** {**rl-1** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **rl-2** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **rl-3** {*packets*| **disable**} [**module** *module*[**port** *start end*]]| **rl-4** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **rl-5** {*packets*| **disable**} [**module** *module* [**port** *start end*]]}| **layer-2** {**l2pt** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **mcast-snooping** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **port-security** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **storm-control** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **vpc-low** {*packets*| **disable**} [**module** *module* [**port** *start end*]]}| **layer-3** {**control** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **glean** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **glean-fast** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **mtu** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **multicast** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| **ttl** {*packets*| **disable**} [**module** *module* [**port** *start end*]]}| **receive** {*packets*| **disable**} [**module** *module* [**port** *start end*]]| || [**portgroup-multiplier** *multiplier* **module** *module*]}

Syntax Description

access-list-log	Specifies packets copied to the supervisor module for access list logging. The default rate is 100 packets per second.
packets	Number of packets per second. The range is from 1 to 33554431.
disable	Disables the rate limiter.
module *module*	(Optional) Specifies a module number. The range is from 1 to 18.
port *start end*	(Optional) Specifies a port start index. The range is from 1 to 32. You specify the start port and and end port with a space in between them.

copy	Specifies data and control packets copied to the supervisor module. The default rate is 30000 packets per second.
f1	Specifies the control packets from the F1 modules to the supervisor.
rl-1	Specifies the F1 rate-limiter 1.
rl-2	Specifies the F1 rate-limiter 2.
rl-3	Specifies the F1 rate-limiter 3.
rl-4	Specifies the F1 rate-limiter 4.
rl-5	Specifies the F1 rate-limiter 5.
layer-2	Specifies Layer 2 packet rate limits.
l2pt	Specifies Layer 2 Tunnel Protocol (L2TP) packets. The default rate is 4096 packets per second.
mcast-snooping	Specifies Layer 2 multicast-snooping packets. The default rate is 10000 packets per second.
port-security	Specifies port security packets. The default is disabled.
storm-control	Specifies broadcast, multicast, and unknown unicast storm-control packets. The default is disabled.
vpc-low	Specifies Layer 2 control packets over the virtual port channel (vPC) low queue. It synchronizes control-plane communication between vPC peer switches that are of a lower priority and protects the control plane when a vPC peer switch misbehaves or excessive traffic occurs between the two. The default rate is 4000 packets per second.
layer-3	Specifies Layer 3 packet rate limits.
control	Specifies Layer-3 control packets. The default rate is 10000 packets per second.
glean	Specifies Layer-3 glean packets. The default rate is 100 packets per second.
glean-fast	Specifies Layer 3 glean fast-path packets. The default rate is 100 packets per second.

mtu	Specifies Layer-3 maximum transmission unit (MTU) failure redirected packets. The default rate is 500 packets per second.
multicast	Specifies Layer-3 multicast packets per second.
ttl	Specifies Layer-3 failed time-to-live redirected packets. The default rate is 500 packets per second.
receive	Specifies packets redirected to the supervisor module. The default rate is 30000 packets per second.
portgroup-multiplier *multiplier*	Specifies the *multiplier* value. The range is from 0.10 to 3.00. The default value is 1.00. **Note** This applies to F2, F2e, and F3 cards.

Command Default

See the Syntax Description for the default rate limits.

Default rate limits for the F1 Series modules:

RL-1: 4500 packets per second

RL-2: 1000 packets per second

RL-3: 1000 packets per second

RL-4: 100 packets per second

RL-5: 1500 packets per second

Command Modes

Global configuration

Command History

Release	Modification
6.2(12)	Added the **portgroup-multiplier** keyword and the *multiplier* parameter.
6.2(2)	Added the **glean-fast** keyword.
5.1(1)	Added the **f1**, **rl-1**, **rl-2**, **rl-3**, **rl-4**, and **rl-5** keywords. Also, added the following keywords: **module**, **disable**, and **port**.
5.0(2)	Added the **l2pt** keyword.
4.1(2)	This command was introduced to replace the **platform rate-limit** command.

Usage Guidelines

Glean fast-path is enabled by default. If glean fast-path programming does not occur due to adjacency resource exhaustion, the system falls back to regular glean programming.

The **hardware rate-limiter layer-3 glean-fast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] command sends packets to the supervisor from F2e, M1, or M2 Series modules.

The **hardware rate-limiter portgroup-multiplier** *multiplier* **module** *module* command applies the *multiplier* to the rate limit. For example, if you configured the ttl rate-limiter as 1000 pps and the multiplier value was 0.5, each ASIC instance would be programmed with 500 pps.

This command does not require a license.

Examples

This example shows how to configure a rate limit for control packets:

```
switch# configure terminal
switch(config)# hardware rate-limiter layer-3 control 20000
```

This example shows how to revert to the default rate limit for control packets:

```
switch# configure terminal
switch(config)# no hardware rate-limiter layer-3 control
```

This example shows how to configure the port group multiplier:

```
switch# configure terminal
switch(config)# hardware rate-limiter portgroup-multiplier 0.5 module 3
```

Related Commands

Command	Description
clear hardware rate-limiter	Clears rate-limit statistics.
show hardware rate-limiter	Displays rate-limit information.
show running-config	Displays the running configuration.

hop-limit

To verify the advertised hop-count limit, use the **hop-limit** command in RA guard policy configuration mode.

hop-limit {**maximum**| **minimum** } *limit*

Syntax Description

maximum *limit*	Verifies that the hop-count limit is lower than that set by the *limit* argument.
minimum *limit*	Verifies that the hop-count limit is greater than that set by the *limit* argument.

Command Default

No hop-count limit is specified.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **hop-limit** command enables verification that the advertised hop-count limit is greater than or less than the value set by the *limit* argument. Configuring the **minimum** *limit* keyword and argument can prevent an attacker from setting a low hop-count limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the **maximum** *limit* keyword and argument enables verification that the advertised hop-count limit is lower than the value set by the *limit* argument. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and sets a minimum hop-count limit of 3:

```
switch(config)# ipv6 nd raguard policy raguard1
switch(config-ra-guard)# hop-limit minimum 3
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

host (IPv4)

To specify a host or a subnet as a member of an IPv4-address object group, use the **host** command. To remove a group member from an IPv4-address object group, use the **no** form of this command.

[*sequence-number*] **host** *IPv4-address*

no {*sequence-number*| **host** *IPv4-address*}

[*sequence-number*] *IPv4-address network-wildcard*

no *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address* / *prefix-len*

no *IPv4-address* / *prefix-len*

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
host *IPv4-address*	Specifies that the group member is a single IPv4 address. Enter *IPv4-address* in dotted-decimal format.
IPv4-address network-wildcard	IPv4 address and network wildcard. Enter *IPv4-address* and *network-wildcard* in dotted-decimal format. Use *network-wildcard* to specify which bits of *IPv4-address* are the network portion of the address, as follows: `switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255` A *network-wildcard* value of 0.0.0.0 indicates that the group member is a specific IPv4 address.
IPv4-address/prefix-len	IPv4 address and variable-length subnet mask. Enter *IPv4-address* in dotted-decimal format. Use *prefix-len* to specify how many bits of *IPv4-address* are the network portion of the address, as follows: `switch(config-ipaddr-ogroup)# 10.23.176.0/24` A *prefix-len* value of 32 indicates that the group member is a specific IP address.

Command Default

None

Command Modes

IPv4 address object group configuration.

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To specify a subnet as a group member, use either of the following forms of this command:

[*sequence-number*] *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address* / *prefix-len*

Regardless of the command form that you use to specify a subnet, the device shows the *IP-address/prefix-len* form of the group member when you use the **show object-group** command.

To specify a single IPv4 address as a group member, use any of the following forms of this command:

[*sequence-number*] **host** *IPv4-address*

[*sequence-number*] *IPv4-address* **0.0.0.0**

[*sequence-number*] *IPv4-address* /**32**

Regardless of the command form that you use to specify a single IPv4 address, the device shows the **host** *IP-address* form of the group member when you use the **show object-group** command.

This command does not require a license.

Examples

This example shows how to configure an IPv4-address object group named ipv4-addr-group-13 with two group members that are specific IPv4 addresses and one group member that is the 10.23.176.0 subnet:

10.121.57.234/32

```
switch# configure terminal
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)#
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
10 host 10.121.57.102
20 host 10.121.57.234
30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

Related Commands

Command	Description
object-group ip address	Configures an IPv4 address group.

Command	Description
show object-group	Displays object groups.

host (IPv6)

To specify a host or a subnet as a member of an IPv6-address object group, use the **host** command. To remove a group member from an IPv6-address object group, use the **no** form of this command.

[*sequence-number*] **host** *IPv6-address*

no {*sequence-number*| **host** *IPv6-address*}

[*sequence-number*] *IPv6-address* /*network-prefix*

no *IPv6-address* /*network-prefix*

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
host *IPv6-address*	Specifies that the group member is a single IPv6 address. Enter *IPv6-address* in colon-separated, hexadecimal format.
IPv6-address /*network-prefix*	IPv6 address and a variable-length subnet mask. Enter*IPv6-address* in colon-separated, hexadecimal format. Use *network-prefix* to specify how many bits of *IPv6-address* are the network portion of the address, as follows: `switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96` A *network-prefix* value of 128 indicates that the group member is a specific IPv6 address.

Command Default

None

Command Modes

IPv6 address object group configuration.

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To specify a subnet as a group member, use the following forms of this command:

[*sequence-number*] *IPv6-address* /*network-prefix*

To specify a single IP address as a group member, use any of the following forms of this command:

[*sequence-number*] **host** *IPv6-address*

[*sequence-number*] *IPv6-address* /*128*

Regardless of the command form that you use to specify a single IPv6 address, the device shows the **host***IPv6-address* form of the group member when you use the **show object-group** command.

This command does not require a license.

Examples

This example shows how to configure an IPv6-address object group named ipv6-addr-group-A7 with two group members that are specific IPv6 addresses and one group member that is the 2001:db8:0:3ab7:: subnet:

10.121.57.234/32

```
switch# configure terminal
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7

10 host 2001:db8:0:3ab0::1
20 host 2001:db8:0:3ab0::2
30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

Related Commands

Command	Description
object-group ipv6 address	Configures an IPv6 address group.
show object-group	Displays object groups.

I Commands

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.

Command Default

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.

Command Default

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.

Command Default

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 interf**ace**	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.

Command Default

None

Command Modes

Global configuration

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.

Command Default

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.

Command	Description
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.

Command Default

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.

Command Default

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.

Command	Description
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.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

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.

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 redirect-response

To enable the DHCP redirect response feature, use the **ip dhcp redirect-response** command on the DHCP server-facing interface. To disable this feature, use the **no** form of this command.

ip dhcp redirect-response

no ip dhcp redirect-response

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

DHCP redirect response feature is supported only on the Cisco M3 Series modules.

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

You can configure the **ip dhcp redirect-response** command on any SVI or L3 interfaces.

Examples

This example shows how to configure DHCP redirect response feature:

```
switch# configure terminal
switch(config)# interface Ethernet 2/1
switch(config-if)# ip dhcp redirect-response
switch(config-if)# end
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP feature.
show running-config dhcp	Displays the DHCP configuration details.

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.

Command Default

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.

Command	Description
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.

Command Default

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.

Command Default

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.

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.
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.

Command Default

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)#
```

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.

Command Default

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# configure terminal
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.

Command Default

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.

Command	Description
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.

Command Default

Disabled

Command Modes

Interface 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.

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 **ipdhcp 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.

Command Default

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.

Command Default

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.

Command	Description
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.

Command Default

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.

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 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.

Command Default

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.

Command	Description
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.

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.

Command Default

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.

Command	Description
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 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.

Command Default

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.

Command	Description
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.

Command Default

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# configure terminal
switch(config)# ip forward-protocol udp
```

This example shows how to disable the UDP relay feature:

```
switch# configure terminal
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.

Command Default

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.
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**.

Command Default

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*

noip 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.

Command Default

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**.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

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.

Command Default

None

Command Modes

Global configuration

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.

Command Default

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# configure terminal
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.

Command	Description
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.

Command Default

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.

Command Default

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 guard policy

To define a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard policy name, use the **ipv6 dhcp guard policy** command in global configuration mode. To remove the DHCPv6 guard policy name, use the **no** form of this command.

ipv6 dhcp guard policy *[policy-name]*

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Default

No DHCPv6 guard policy name is defined.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

This command allows you to enter DHCPv6 guard configuration mode. DHCPv6 guard policies can be used to block reply and advertisement messages that come from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.

Examples

The following example shows how to define a DHCPv6 guard policy name:

```
switch# configure terminal
switch(config)# ipv6 dhcp guard policy policy1
```

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.

Command Default

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 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.

Command Default

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 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.

Command Default

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.

Command Default

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 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.

Command Default

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 nd raguard attach-policy

To apply the IPv6 router advertisement (RA) guard feature on a specified interface, use the **ipv6 nd raguard attach-policy** command in interface configuration mode.

ipv6 nd raguard attach-policy [*policy-name* [**vlan** {**add**| **except**| **none**| **remove**| **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

Syntax Description

policy-name	(Optional) IPv6 RA guard policy name.
vlan	(Optional) Applies the IPv6 RA guard feature to a VLAN on the interface.
add	Adds a VLAN to be inspected.
except	All VLANs are inspected except the one specified.
none	No VLANs are inspected.
remove	Removes the specified VLAN from RA guard inspection.
all	ND traffic from all VLANs on the port is inspected.
vlan	(Optional) A specific VLAN on the interface. More than one VLAN can be specified (*vlan1*, *vlan2*, *vlan3*...). The range of available VLAN numbers is from 1 through 4094.

Command Default

An IPv6 RA guard policy is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

If no policy is specified using the *policy-name* argument, the port device role is set to host and all inbound router traffic (for example, RA and redirect messages) is blocked.

If no VLAN is specified (which is equal to entering the **vlan all** keywords after the *policy-name* argument), RA guard traffic from all VLANs on the port is analyzed.

If specified, the VLAN parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated vlan parameters or in dash-specified ranges; for example, vlan 1-100,200,300-400.

Examples

In the following example, the IPv6 RA guard feature is applied on GigabitEthernet interface 0/0:

```
switch(config)# interface GigabitEthernet 0/0
switch(config-if)# ipv6 nd raguard attach-policy
```

ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd raguard policy** command in global configuration mode.

ipv6 nd raguardpolicy *policy-name*

Syntax Description

policy-name	IPv6 RA guard policy name.

Command Default

An RA guard policy is not configured.

Command Modes

Global configuration (config)#

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

Use the **ipv6 nd raguard policy** command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd raguard attach-policy** command to enable IPv6 RA guard on a specific interface.

Examples

The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:

```
switch(config)# ipv6 nd raguard policy policy1
switch(config-ra-guard)#
```

Related Commands

Command	Description
device-role	Specifies the role of the device attached to the port.
ipv6 nd raguard attach-policy	Applies the IPv6 RA guard feature on a specified interface.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link layer address.

ipv6 neighbor binding

To change the defaults of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command in global configuration mode. To return the networking device to its default, use the **no** form of this command.

ipv6 neighbor binding [**reachable-lifetime** *value*| **stale-lifetime** *value*]

no ipv6 neighbor binding

Syntax Description

reachable-lifetime *value*	(Optional) The maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 through 3600 seconds, and the default is 300 seconds (or 5 minutes).
stale-lifetime *value*	(Optional) The maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. • The default is 24 hours (86,400 seconds).
down-lifetime *value*	(Optional) The maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. • The default is 24 hours (86,400 seconds).

Command Default

Reachable lifetime: 300 seconds Stale lifetime: 24 hours Down lifetime: 24 hours

Command Modes

Global configuration (config)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding** command to configure information about individual entries in a binding table. If no keywords or arguments are configured, the IPv6 neighbor binding entry defaults are used.

If the **tracking reachable-lifetime** command is configured, it overrides **ipv6 neighbor binding reachable-lifetime** configuration. If the **tracking stale-lifetime** command is configured, it overrides **ipv6 neighbor binding stale-lifetime** configuration.

Examples

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
switch(config)# ipv6 neighbor binding reachable-entries 100
```

Related Commands

Command	Description
ipv6 neighbor tracking	Tracks entries in the binding table.
tracking	Overrides the default tracking policy on a port.

ipv6 neighbor binding logging

To enable the logging of binding table main events, use the **ipv6 neighbor binding logging** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 neighbor binding logging

no ipv6 neighbor binding logging

Syntax Description

This command has no arguments or keywords.

Command Default

Binding table events are not logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 neighbor binding logging** command enables the logging of the following binding table events:

- An entry is inserted into the binding table.
- A binding table entry was updated.
- A binding table entry was deleted from the binding table.
- A binding table entry was not inserted into the binding table, possibly because of a collision with an existing entry, or because the maximum number of entries has been reached.

Examples

The following example shows how to enable binding table event logging:

```
switch(config)# ipv6 neighbor binding logging
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.
ipv6 snooping logging packet drop	Configures IPv6 snooping security logging.

ipv6 neighbor binding max-entries

To specify the maximum number of entries that are allowed to be inserted in the binding table cache, use the **ipv6 neighbor binding max-entries** command in global configuration mode. To return to the default, use the **no** form of this command.

ipv6 neighbor binding max-entries *entries* [**vlan-limit** *number*| **interface-limit** *number*| **mac-limit** *number*]

no ipv6 neighbor binding max-entries *entries* [**vlan-limit**| **mac-limit**]

Syntax Description

entries	Number of entries that can be inserted into the cache.
vlan-limit *number*	(Optional) Specifies a neighbor binding limit per number of VLANs.
interface-limit *number*	(Optional) Specifies a neighbor binding limit per interface.
mac-limit *number*	(Optional) Specifies a neighbor binding limit per number of Media Access Control (MAC) addresses.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 neighbor binding max-entries** command is used to control the content of the binding table. This command specifies the maximum number of entries that are allowed to be inserted in the binding table cache. Once this limit is reached, new entries are refused, and the Neighbor Discovery Protocol (NDP) traffic source with the new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in the database, no entries are cleared, and the new threshold is reached after normal cache attrition.

The maximum number of entries can be set globally per VLAN, interface, or MAC addresses.

Examples

The following example shows how to specify globally the maximum number of entries inserted into the cache:

```
switch(config)# ipv6 neighbor binding max-entries 100
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor tracking

To track entries in the binding table, use the **ipv6 neighbor tracking** command in global configuration mode. To disable entry tracking, use the **no** form of this command.

ipv6 neighbor tracking [**retry-interval** *value*]

no ipv6 neighbor tracking [**retry-interval** *value*]

Syntax Description

retry-interval *value*	(Optional) Verifies a static entry's reachability at the configured interval time, in seconds, between two probings. The range is from 1 to 3600, and the default is 300.

Command Default

Entries in the binding table are not tracked.

Command Modes

Global configuration (config)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 neighbor tracking** command enables the tracking of entries in the binding table. Entry reachability is tested at every interval configured by the optional **retry-interval** keyword (or every 300 seconds, which is the default retry interval) using the neighbor unreachability detection (NUD) mechanism used for directly tracking neighbor reachability.

Reachability can also be established indirectly by using Neighbor Discovery Protocol (NDP) inspection up to the VERIFY_MAX_RETRIES value (the default is 10 seconds). When there is no response, entries are considered stale and are deleted after the stale lifetime value is reached (the default is 1440 minutes).

When the **ipv6 neighbor tracking** command is disabled, entries are considered stale after the reachable lifetime value is met (the default is 300 seconds) and deleted after the stale lifetime value is met.

To change the default values of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command.

Examples

The following example shows how to track entries in a binding table:

```
switch(config)# ipv6 neighbor tracking
```

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

ipv6 port traffic-filter

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

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

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

Syntax Description

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

Command Default

None

Command Modes

Interface configuration

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.

Command	Description
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.
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 snooping attach-policy

To apply an IPv6 snooping policy to a target, use the **ipv6 snooping attach-policy** command in IPv6 snooping configuration mode, or interface configuration mode. To remove a policy from a target, **no** form of this command.

ipv6 snooping attach-policy *policy-name*

Syntax Description

policy-name	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 snooping policy is not attached to a target.

Command Modes

IPv6 snooping configuration (config-ipv6-snooping)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

Once a policy has been identified or configured, it is applied on a target using the **ipv6 snooping attach-policy** command. This command is applied on any target, which varies depending on the platform. Examples of targets (depending on the platform used) include device ports, switchports, Layer 2 interfaces, Layer 3 interfaces, and VLANs.

Examples

The following examples shows how to apply an IPv6 snooping policy named policy1 to a target:

```
switch(config)# ipv6 snooping policy policy1
switch(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
```

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.

Command Default

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.

K Commands

key

To create a key or to enter the configuration mode for an existing key, use the **key** command. To remove the key, use the **no** form of this command.

key *key-ID*

no key *key-ID*

Syntax Description

key-ID	ID of the key to be configured. This ID must be a whole number between 0 and 65535. **Note** The MACsec key identifier must range from 1 to 32 octet, and the maximum size is 64 characters.

Command Default

None

Command Modes

Keychain configuration (config-keychain)

MACsec keychain configuration (config-macseckeychain)

Command History

Release	Modification
8.2(1)	This command was modified. Support for the MACsec keychain configuration mode was added.
4.0(1)	This command was introduced.

Usage Guidelines

- A new key contains no key strings.
- This command does not require a license.
- To use this command in MACsec keychain configuration mode, you should enable the MKA feature first.

Examples

This example shows how to enter the key configuration mode for key 13 in the glbp-keys keychain:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)#
```

This example shows how to enter the MACsec key configuration mode for key 01 in the k1 MACsec keychain:

```
switch# configure terminal
switch(config)# key chain k1 macsec
switch(config-macseckeychain)# key 01
switch(config-macseckeychain-macseckey)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
feature mka	Enables the MKA feature.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
key-octet-string	Configures the text for a MACsec key.
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
key-string	Configures the shared secret (text) for a specific key.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
send-lifetime	Configures a send lifetime for a key.
show key chain	Displays keychain configuration.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

key chain

To create a keychain or to configure an existing keychain, use the **key chain** command. To unconfigure the keychain, use the **no** form of this command.

key chain *keychain-name* **[macsec]**

no key chain *keychain-name* **[macsec]**

Syntax Description

key chain *keychain-name*	Specifies the name of the keychain. The maximum size is 63 alphanumeric characters. It is case sensitive.
macsec	(Optional) Configures the MACsec keychain.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
8.2(1)	This command was modified. The **macsec** keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

- This command creates a keychain if it does not already exist. A new keychain contains no keys. Note that removing a keychain also removes the keys that are a part of this keychain. Before you remove a keychain, ensure that no feature is using it. If a feature is configured to use a keychain that you remove, that feature is likely to fail to communicate with other devices.
- This command does not require a license.
- To configure a MACsec keychain, you should enable the MKA feature first.

Examples

This example shows how to configure a keychain named glbp-keys:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)#
```

This example shows how to configure a MACsec key chain named k1:

```
switch# configure terminal
switch(config)# key chain k1 macsec
switch(config-macseckeychain)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
feature mka	Enables the MKA feature.
key	Configures a key.
key-octet-string	Configures the text for a MACsec key.
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
key-string	Configures a key string.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
send-lifetime	Configures a send lifetime for a key.
show key chain	Displays the keychain configuration.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

key config-key

To configure the master key for type-6 encryption, use the **key config-key** command. To delete the master key and stop type-6 encryption, use the **no** form of this command.

key config-key ascii *new-master-key*

no key config-key ascii

Syntax Description

ascii	Specifies the ASCII format.
new-master-key	The master key. The master key can be a minimum of 16 to a maximum of 32 alphanumeric characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the master key for type-6 encryption:

```
switch# key config-key ascii

New Master Key:
Retype Master Key:
```

This example shows how to delete the master key and stop type-6 encryption:

```
switch# no key config-key ascii

Warning deletion of master-key will stop further type-6 encryption.
Do you want to proceed (y/n)[n]: [n] y
switch#
```

Related Commands

Command	Description
feature password encryption aes	Enables the AES password encryption features.
show encryption service stat	Displays the status of the encryption service.

key-octet-string

To configure the text for a MACsec key, use the **key-octet-string** command. To remove the text, use the **no** form of this command.

key-octet-string [**0** | **7**] *key-octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**}

no key-octet-string [**0** | **7**] *key-octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**}

Syntax Description

0	(Optional) Specifies the type of encryption to use. The *key-octet-string* argument that you enter is unencrypted text.
7	(Optional) Specifies the type of encryption to use. The *key-octet-string* argument that you enter is encrypted. The encryption method is a Cisco-proprietary method. This option is useful when you are entering a text string based on the encrypted output of the **show key chain** command that you run on another Cisco NX-OS device.
key-octet-string	Text of the key octet string. The text is alphanumeric, case sensitive, and can have up to 64 characters. **Note** The text can have up to 130 characters for encryption type 7.
cryptographic-algorithm	Specifies the Cipher-based Message Authentication Code (CMAC) algorithm for authentication.
AES_128_CMAC	Configures the 128-bit AES encryption algorithm.
AES_256_CMAC	Configures the 256-bit AES encryption algorithm.

Command Default

The key octet string is not encrypted.

Command Modes

MACsec key configuration (config-macseckeychain-macseckey)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

The key octet string is a shared secret. The device stores key strings in a secure format. You can obtain encrypted key strings by using the **show key chain** command on another Cisco NX-OS device. This command does not require a license. To use this command, you must enable the MKA feature.

Examples

This example shows how to set a key octet string:

```
switch# configure terminal
switch(config)# key chain k1 macsec
switch(config-macseckeychain)# key 03
switch(config-macseckeychain-macseckey)# key-octet-string 0123456789aabbcc0123456789aabbcc
 cryptographic-algorithm AES_128_CMAC
switch(config-macseckeychain-macseckey)#
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

key-server-priority

To configure the preference for a device to serve as the key server for MACsec Key Agreement (MKA) encryption, use the **key-server-priority** command. To reset the default preference, use the **no** form of this command.

key-server-priority *value*

no key-server-priority *value*

Syntax Description

value	Priority for a device to become the key server. The lower the value, the higher the preference. The range is from 0 to 255.

Command Default

16

Command Modes

MACsec policy configuration (config-macsec-policy)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, enable the MKA feature.

Examples

This example shows how to set the key server priority:

```
switch# configure terminal
switch(config)# macsec policy p1
switch(config-macsec-policy)# key-server-priority 9
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
macsec keychain policy	Configures the MACsec keychain policy.

Command	Description
macsec policy	Configures the MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

key-string

To configure the text for a key, use the **key-string** command. To remove the text, use the **no** form of this command.

key-string [*encryption-type*] *text-string*

no key-string *text-string*

Syntax Description

encryption-type	(Optional) Type of encryption to use. The *encryption-type* argument can be one of the following values: • 0—The text-string argument that you enter is unencrypted text. This is the default. • 7—The text-string argument that you enter is encrypted. The encryption method is a Cisco proprietary method. This option is useful when you are entering a text string based on the encrypted output of a **show key chain** command that you ran on another Cisco NX-OS device.
text-string	Text of the key string, up to 63 case-sensitive, alphanumeric characters. The value of the first 2 digits of a type 7 key string configured by using the **key-string 7** *text-string* command has to be between 0 and 15. For example, you can configure 07372b557e2c1a as the key string value in which case the sum value of the first 2 digits will be 7. But, you cannot configure 85782916342021 as the key string value because the value of the first 2 digits will be 85. We recommend unconfiguring any type 7 key strings that do not adhere to this value or to configure a type 0 string.

Command Default

None

Command Modes

Key configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The key-string text is a shared secret. The device stores key strings in a secure format.

You can obtain encrypted key strings by using the **show key chain** command on another Cisco NX-OS device.

This command does not require a license.

Examples

This example shows how to enter an encrypted shared secret for key 13:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# key-string 7 071a33595c1d0c1702170203163e3e21213c20361a021f11
switch(config-keychain-key)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
key	Configures a key.
key chain	Configures a keychain.
send-lifetime	Configures a send lifetime for a key.
show key chain	Shows keychain configuration.

L Commands

ldap-server deadtime

To configure the deadtime interval for all Lightweight Directory Access Protocol (LDAP) servers, use the **ldap-server deadtime** command. The deadtime interval specifies the time that the Cisco NX-OS device waits, after declaring that an LDAP server is dead, before sending out a test packet to determine if the server is now alive. To remove the global deadtime interval configuration, use the **no** form of this command.

ldap-server deadtime *minutes*

no ldap-server deadtime *minutes*

Syntax Description

minutes	Global deadtime interval for LDAP servers. The range is from 1 to 60 minutes.

Command Default

0 minutes

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

When the dead-time interval is 0 minutes, LDAP servers are not marked as dead even if they are not responding.

This command does not require a license.

Examples

This example shows how to configure the global deadtime interval for LDAP servers:

```
switch# configure terminal
switch(config)# ldap-server deadtime 5
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server host

To configure Lightweight Directory Access Protocol (LDAP) server host parameters, use the **ldap-server host** command. To revert to the defaults, use the **no** form of this command.

ldap-server host {*ipv4-address*| *ipv6-address*| *host-name*} **[enable-ssl]** [**port** *tcp-port* [**timeout** *seconds*]] [**rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*]| [**timeout seconds**]]] [**test rootDN** *root-name* [**idle-time** *minutes*| **password** *password* [**idle-time** *minutes*]| **username** *name* [**password** *password* [**idle-time** *minutes*]]]] [**timeout** *seconds*]

noldap-server host {*ipv4-address*| *ipv6-address*| *host-name*} **[enable-ssl]** [**port** *tcp-port* [**timeout** *seconds*]] [**rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*]| [**timeout seconds**]]] [**test rootDN** *root-name* [**idle-time** *minutes*| **password** *password* [**idle-time** *minutes*]| **username** *name* [**password** *password* [**idle-time** *minutes*]]]] [**timeout** *seconds*]

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X:X* format.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
enable-ssl	(Optional) Ensures the integrity and confidentiality of the transferred data by causing the LDAP client to establish a Secure Sockets Layer (SSL) session before sending the bind or search request.
port *tcp-port*	(Optional) Specifies the TCP port to use for LDAP messages to the server. The range is from 1 to 65535.
timeout *seconds*	(Optional) Specifies the timeout interval for the server. The range is from 1 to 60 seconds.
rootDN *root-name*	(Optional) Specifies the root designated name (DN) for the LDAP server database. You can enter up to 128 alphanumeric characters for the root name.
password *password*	(Optional) Specifies the bind password for the root.
test	(Optional) Configures parameters to send test packets to the LDAP server.
idle-time *minutes*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.

username *name*	Specifies a username in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters. **Note** To protect network security, we recommend that you use a username that is not the same as an existing username in the LDAP database.

Command Default

Server monitoring: Disabled.

TCP port: The global value or 389 if a global value is not configured.

Timeout: The global value or 5 seconds if a global value is not configured.

Idle time: 60 minutes.

Test username: test.

Test password: Cisco

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP and obtain the IPv4 or IPv6 address or hostname for the remote LDAP server.

If you plan to enable the SSL protocol, make sure that the LDAP server certificate is manually configured on the Cisco NX-OS device.

By default, when you configure an LDAP server IP address or hostname on the Cisco NX-OS device, the LDAP server is added to the default LDAP server group. You can also add the LDAP server to another LDAP server group.

The timeout interval value specified for an LDAP server overrides the global timeout interval value specified for all LDAP servers.

This command does not require a license.

Examples

This example shows how to configure the IPv6 address for an LDAP server:

```
switch# configure terminal
switch(config)# ldap-server host 10.10.2.2 timeout 20
```

This example shows how to configure the parameters for LDAP server monitoring:

```
switch# configure terminal
switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password Ur2Gd2BH
 idle-time 3
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server port

To configure a global Lightweight Directory Access Protocol (LDAP) server port through which clients initiate TCP connections, use the **ldap-server port** command. To remove the LDAP server port configuration, use the **no** form of this command.

ldap-server port *tcp-port*

no ldap-server port *tcp-port*

Syntax Description

tcp-port	Global TCP port to use for LDAP messages to the server. The range is from 1 to 65535.

Command Default

TCP port 389

Command Modes

Global configuration

Command History

Release	Modification
5.2(1)	This command was deprecated.
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure a global TCP port for LDAP messages:

```
switch# configure terminal
switch(config)# ldap-server port 2
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server timeout

To configure a global timeout interval that determines how long the Cisco NX-OS device waits for responses from all Lightweight Directory Access Protocol (LDAP) servers before declaring a timeout failure, use the **ldap-server timeout** command. To remove the global timeout configuration, use the **no** form of this command.

ldap-server timeout seconds

no ldap-server timeout seconds

Syntax Description

seconds	Timeout interval for LDAP servers. The range is from 1 to 60 seconds.

Command Default

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the global timeout interval for LDAP servers:

```
switch# configure terminal
switch(config)# ldap-server timeout 10
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap search-map

To configure a Lightweight Directory Access Protocol (LDAP) search map to send a search query to the LDAP server, use the **ldap search-map** command. To disable the search map, use the **no** form of this command.

ldap search-map *map-name*

no ldap search-map *map-name*

Syntax Description

map-name	Name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure an LDAP search map:

```
switch# configure terminal
switch(config)# ldap search-map map1
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-search-map	Displays the configured LDAP search maps.
CRLLookup	Configures the attribute name, search filter, and base-DN for the CRL search operation in order to send a search query to the LDAP server.

Command	Description
trustedCert	Configures the attribute name, search filter, and base-DN for the trusted certificate search operation in order to send a search query to the LDAP server.
user-certdn-match	Configures the attribute name, search filter, and base-DN for the certificate DN match search operation in order to send a search query to the LDAP server.
user-pubkey-match	Configures the attribute name, search filter, and base-DN for the public key match search operation in order to send a search query to the LDAP server.
user-switch-bind	Configures the attribute name, search filter, and base-DN for the user-switchgroup search operation in order to send a search query to the LDAP server.
userprofile	Configures the attribute name, search filter, and base-DN for the user profile search operation in order to send a search query to the LDAP server.

logging drop threshold

To configure the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold in a policy map for Control Plane Policing (CoPP), use the **logging drop threshold** command.

logging drop threshold [*drop-count* [**level** *syslog-level*]]

Syntax Description

drop-count	Drop count. The range is from 1 to 80000000000.
level	(Optional) Specifies the syslog level.
syslog-level	Syslog level. The range is from 1 to 7.

Command Default

Syslog level 5

Command Modes

config-pmap-c

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

Ensure that you are in the default VDC.

Ensure that you have configured the IP ACLs if you want to use ACE hit counters in the class maps.

This command does not require a license.

Examples

This example shows how to configure the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold in a policy map for CoPP:

```
switch# configure terminal
switch(config)# policy-map type control-plane ClassMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# police cir 52000
switch(config-pmap-c)# police cir 52000 bc 2000
switch(config-pmap-c)# police cir 5000 conform transmit exceed drop violate set1 dscp3 dscp4
 table1 pir-markdown-map
switch(config-pmap-c)# police cir 52000 pir 78000 be 2000
switch(config-pmap-c)# logging drop threshold 1800 level 2
switch(config-pmap-c)#
```

Related Commands

Command	Description
policy-map type control-plane	Configures a control plane policy map and enters policy map configuration mode.

lt

To specify a less-than group member for an IP port object group, use the **lt** command. A less-than group member matches port numbers that are less than (and not equal to) the port number specified in the entry. To remove a greater-than group member from port object group, use the **no** form of this command.

[*sequence-number*] **lt** *port-number*

no {*sequence-number*| **lt** *port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
port-number	Port number that traffic matching this group member does not exceed or equal. Valid values are from 0 to 65535.

Command Default

None

Command Modes

IP port object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether a **lt** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 1 through port 49151:

```
switch# configure terminal
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# lt 49152
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.
object-group ip port	Configures an IP port object group.
range	Specifies a port range group member in an IP port object group.
show object-group	Displays object groups.

M Commands

mac access-list

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

mac access-list *access-list-name*

no mac access-list *access-list-name*

Syntax Description

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

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

No MAC ACLs are defined by default.

Use MAC ACLs to filter non-IP traffic. If you disable packet classification, you can use MAC ACLs to filter all traffic.

When you use the **mac access-list** command, the device enters MAC access list configuration mode, where you can use the MAC **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 **mac port access-group** command to apply the ACL to an interface.

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

```
deny any any
protocol
```

This implicit rule ensures that the device denies the unmatched traffic, regardless of the protocol specified in the Layer 2 header of the traffic.

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

This command does not require a license.

Examples

This example shows how to enter MAC access list configuration mode for a MAC ACL named mac-acl-01:

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

Related Commands

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

mac packet-classify

To enable MAC packet classification on a Layer 2 interface, use the **mac packet-classify** command. To disable MAC packet classification, use the **no** form of this command.

mac packet-classify

no mac packet-classify

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

MAC packet classification allows you to control whether a MAC ACL that is on a Layer 2 interface applies to all traffic entering the interface, including IP traffic, or to non-IP traffic only.

When MAC packet classification is enabled on a Layer 2 interface, a MAC ACL that is on the interface applies to all traffic entering the interface, including IP traffic. Also, you cannot apply an IP port ACL on the interface.

When MAC packet classification is disabled on a Layer 2 interface, a MAC ACL that is on the interface applies only to non-IP traffic entering the interface. Also, you can apply an IP port ACL on the interface.

To configure an interface as a Layer 2 interface, use the **switchport** command.

Examples

This example shows how to configure an Ethernet interface to operate as a Layer 2 interface and to enable MAC packet classification:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# switchport
switch(config-if)# mac packet-classify
switch(config-if)#
```

This example shows how to view the configuration of an Ethernet interface and the error message that appears if you try to apply an IP 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 port access-group	Applies a IPv4 ACL to an interface as a port ACL.
ipv6 port traffic-filter	Applies a IPv6 ACL to an interface as a port ACL.
switchport	Configures an interface to operate as a Layer 2 interface.

mac port access-group

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

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

Syntax Description

access-list-name	Name of the MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

MAC ACLs apply to non-IP traffic, unless the device is configured to not classify traffic based on Layer 3 headers. If packet classification is disabled, MAC ACLs apply to all traffic.

You can use the **mac port access-group** command to apply a MAC ACL as a port ACL to the following interface types:

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

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

The device applies MAC ACLs only to inbound traffic. When the device applies a MAC ACL, the device checks 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 a MAC ACL named mac-acl-01 to Ethernet interface 2/1:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# mac port access-group mac-acl-01
```

This example shows how to remove a MAC ACL named mac-acl-01 from Ethernet interface 2/1:

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

Related Commands

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

macsec keychain policy

To apply a MACsec policy on an interface or port channel, use the **macsec keychain policy** command. To disable the policy on the interface or the port channel, use the **no** form of this command.

macsec keychain *keychain-name* **policy** *policy-name*

nomacsec keychain *keychain-name* **policy** *policy-name*

Syntax Description

keychain-name	Specifies the name of the keychain. The maximum size is 63 alphanumeric characters. It is case sensitive.

Command Default

The **system-default-macsec-policy** default policy is used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, you should enable the MKA feature first.

Examples

This example shows how to apply a MACsec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 11/31
switch(config-if)# macsec keychain k3 policy p1
```

This example shows how to apply a MACsec policy on a port channel:

```
switch# configure terminal
switch(config)# interface port 5
switch(config-if)# macsec keychain k3 policy p1
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.

Command	Description
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
macsec policy	Configures the MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

macsec policy

To configure a MACsec policy, use the **macsec policy** *policy-name* command. To disable the policy, use the **no** form of this command.

macsec policy *policy-name*

no macsec policy *policy-name*

Syntax Description

policy-name	Specifies the policy name. It can be alphanumeric.

Command Default

The **system-default-macsec-policy** default policy is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, you should enable the MKA feature first.

Examples

This example shows how to configure a MACsec policy:

```
switch# configure terminal
switch(config)# macsec policy p1
```

Related Commands

Command	Description
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
macsec keychain policy	Configures the MACsec keychain policy.
show key chain	Displays the configuration of the specified keychain.

Command	Description
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

managed-config-flag

To verify the advertised managed address configuration parameter, use the **managed-config-flag** command in RA guard policy configuration mode.

managed-config-flag {**on**| **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **managed-config-flag** command enables verification of the advertised managed address configuration parameter (or "M" flag). This flag could be set by an attacker to force hosts to obtain addresses through a DHCPv6 server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables M flag verification:

```
switch(config)# ipv6 nd raguard policy raguard1
switch(config-ra-guard)# managed-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

match (class-map)

To configure match criteria for control place class maps, use the **match** command. To delete match criteria for a control plane policy map, use the **no** form of the command.

match access-group name *access-list*

match exception [**ip** [**unicast rpf-failure**]| **ipv6**] {**icmp** {**redirect**| **unreachable**}| **option**}

match protocol arp

match redirect {**arp-inspect**| **dhcp-snoop**}

no match access-group name *access-list*

no match exception [**ip** [**unicast rpf-failure**]| **ipv6**] {**icmp** {**redirect**| **unreachable**}| **option**}

no match protocol arp

no match redirect {**arp-inspect**| **dhcp-snoop**}

Syntax Description

access-group name *access-list*	Matches an IP or MAC access control list.
exception	Matches exception packets.
ip	(Optional) Matches IPv4 exception packets.
ipv6	(Optional) Matches IPv6 exception packets.
unicast rpf-failure	(Optional) Matches IPv4 Unicast Reverse Path Forwarding (Unicast RPF) packets.
icmp	Matches IPv4 or IPv6 ICMP packets.
redirect	Matches IPv4 or IPv6 ICMP redirect packets.
unreachable	Matches IPv4 or IPv6 ICMP unreachable packets.
option	Matches IPv4 or IPv6 option packets.
protocol arp	Matches Address Resolution Protocol (ARP) packets.
redirect	Matches dynamic ARP inspection or DHCP snooping redirect packets.
arp-inspect	Matches dynamic ARP inspection.
dhcp-snoop	Matches dynamic DHCP snooping.

Command Default

None

Command Modes

Class map configuration

Command History

Release	Modification
6.2(10)	The **unicast rpf-failure** keywords were added.
4.0(3)	Added support for policing IPv6 packets.
4.0(1)	This command was introduced.

Usage Guidelines

You must create the IP ACLs or MAC ACLs before you reference them in this command.

You can use this command only in the default VDC.

This command does not require a license.

Examples

This example shows how to specify a match criteria for a control plane class map:

```
switch# configure terminal
switch(config)# class-map type control-plane ClassMapA
switch(config-pmap)# match exception ip icmp redirect
switch(config-pmap)# match redirect arp-inspect
```

This example shows how to remove a criteria for a control plane class map:

```
switch# configure terminal
switch(config)# class-map type control-plane ClassMapA
switch(config-pmap)# no match exception ip icmp redirect
```

Related Commands

Command	Description
class-map type control-plane	Creates or specifies a control plane class map and enters class map configuration mode.
show class-map type control-plane	Displays configuration information for control plane policy maps.

match (VLAN access-map)

To specify an access control list (ACL) for traffic filtering in a VLAN access map, use the **match** command. To remove a **match** command from a VLAN access map, use the **no** form of this command.

match {**ip**| **ipv6**| *mac*} **address** *access-list-name*

no match {**ip**| **ipv6**| **mac**} **address** *access-list-name*

Syntax Description

ip	Specifies that the ACL is an IPv4 ACL.
ipv6	Specifies that the ACL is an IPv6 ACL.
mac	Specifies that the ACL is a MAC ACL.
address *access-list-name*	Specifies the ACL by name, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

VLAN access-map configuration

Command History

Release	Modification
4.1(2)	The **ipv6** keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

You can specify one or more **match** commands per entry in a VLAN access map.

By default, the device classifies traffic and applies IPv4 ACLs to IPv4 traffic, IPv6 ACLs to IPv6 traffic, and MAC ACLs to all other traffic.

This command does not require a license.

Examples

This example shows how to create a VLAN access map named vlan-map-01 and add two entries that each have two **match** commands and one **action** command:

```
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# match mac address mac-acl-00f
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-320
switch(config-access-map)# match mac address mac-acl-00e
switch(config-access-map)# action drop
switch(config-access-map)# show vlan access-map
Vlan access-map vlan-map-01 10

        match ip: ip-acl-01
        match mac: mac-acl-00f
        action: forward
Vlan access-map vlan-map-01 20
        match ip: ip-acl-320
        match mac: mac-acl-00e
        action: drop
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

monitor session

To configure an access control list (ACL) capture session in order to selectively monitor traffic on an interface or VLAN, use the **monitor session** command.

monitor session *session* **type acl-capture**

Syntax Description

session	Session ID. The range is from 0 to 48.
type	Specifies a session type.
acl-capture	Creates an ACL capture session.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an ACL capture session:

```
switch# configure terminal
switch(config)# monitor session 5 type acl-capture
switch(config-acl-capture)#
```

Related Commands

Command	Description
access-list capture	Enables access control list (ACL) capture on all virtual device contexts (VDCs).
destination interface	Configures a destination for ACL capture packets.
show ip-access capture session	Displays the ACL capture session configuration.

N Commands

nac enable

To enable Network Admission Control (NAC) on an interface, use the **nac enable** command. To disable NAC, use the **no** form of this command.

nac enable

no nac enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature eou** command and set the switchport mode to access before using the **nac enable** command.

You can enable EAPoUDP only on an access mode interface.

This command does not require a license.

Examples

This example shows how to enable NAC on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# nac enable
```

This example shows how to disable NAC on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no nac enable
```

Related Commands

Command	Description
feature eou	Enables EAPoUDP.
show eou	Displays EAPoUDP information.

neq

To specify a not-equal-to group member for an IP port object group, use the **neq** command. To remove a not-equal-to group member from port object group, use the **no** form of this command.

[*sequence-number*] **neq** *port-number*

no {*sequence-number*| **neq** *port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
port-number	Port number that this group member does not match. Valid values are from 0 to 65535.

Command Default

None

Command Modes

IP port object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A not-equal-to group member matches port numbers that are not equal to the port number specified in the entry.

IP port object groups are not directional. Whether an **neq** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to any port except port 80:

```
switch# configure terminal
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# neq 80
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.
object-group ip port	Configures an IP port object group.
range	Specifies a port-range group member in an IP port object group.
show object-group	Displays object groups.

O Commands

object-group (identity policy)

To specify a MAC access control list (ACL) for an identity policy, use the **object-group** command. To remove ACL from the identity policy, use the **no** form of this command.

object-group *acl-name*

no object-group *acl-name*

Syntax Description

acl-name	Name of a MAC ACL. The name is case sensitive.

Command Default

None

Command Modes

Identity policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **mac access-list** command to create the MAC ACL to assign to the identity policy.

This command does not require a license.

Examples

This example shows how to configure an ACL for an identity policy:

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

This example shows how to remove an ACL from an identity policy:

```
switch# configure terminal
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# no object-group
```

Related Commands

Command	Description
identity policy	Creates or specifies an identity policy and enters identity policy configuration mode.
mac access-list	Creates a MAC ACL and enters MAC ACL configuration mode.
show identity policy	Displays identity policy information.

object-group ip address

To define an IPv4 address object group or to enter object-group configuration mode for a specific IPv4-address object group, use the **object-group ip address** command. To remove an IPv4-address object group, use the **no** form of this command.

object-group ip address *name*

no object-group ip address *name*

Syntax Description

name	Name of the IPv4 address object group, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use IPv4 object groups in **permit** and **deny** commands for IPv4 access control lists (ACLs).

IPv4 address object groups are not directional. Whether group members match a source or destination address or whether an object group applies to inbound or outbound traffic depends upon how you use the object group in an IPv4 ACL.

This command does not require a license.

Examples

This example shows how to configure an IPv4 address object group named ipv4-addr-group-13 with two group members that are specific IPv4 addresses and one group member that is the 10.23.176.0 subnet:

```
switch# configure terminal
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)# 10.121.57.234/32
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
        10 host 10.121.57.102
        20 host 10.121.57.234
        30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

Related Commands

Command	Description
host (IPv4)	Configures a group member for an IPv4 address object group.
show object-group	Displays object groups.

object-group ip port

To define an IP port object group or to enter object-group configuration mode for a specific IP port object group, use the **object-group ip port** command. To remove an IP port object group, use the **no** form of this command.

object-group ip port *name*

no object-group ip port *name*

Syntax Description

name	Name of the IP port object group, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use IP port object groups in **permit** and **deny** commands for IPv4 and IPv6 access control lists (ACLs).

IP port object groups are not directional. Whether group members match a source or destination port or whether an object group applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 443:

```
switch# configure terminal
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# eq 443
switch(config-port-ogroup)# show object-group
port-group-05
        10 eq 443
switch(config-port-ogroup)#
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.
range	Specifies a port range group member in an IP port object group.
show object-group	Displays object groups.

object-group ipv6 address

To define an IPv6 address object group or to enter IPv6 address object group configuration mode for a specific IPv6 address object group, use the **object-group ipv6 address** command. To remove an IPv6 address object group, use the **no** form of this command.

object-group ipv6 address *name*

no object-group ipv6 address *name*

Syntax Description

name	Name of the IPv6 address group object, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use IPv6 object groups in **permit** and **deny** commands for IPv6 ACLs.

IPv6 address object groups are not directional. Whether group members match a source or destination address or whether an object group applies to inbound or outbound traffic depends upon how you use the object group in an IPv6 ACL.

This command does not require a license.

Examples

This example shows how to configure an IPv6 address object group named ipv6-addr-group-A7 with two group members that are specific IPv6 addresses and one group member that is the 2001:db8:0:3ab7:: subnet:

```
switch# configure terminal
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group i
pv6-addr-group-A7
        10 host 2001:db8:0:3ab0::1
        20 host 2001:db8:0:3ab0::2
        30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

Related Commands

Command	Description
host (IPv6)	Configures a group member for an IPv6 address object group.
show object-group	Displays object groups.

object-group udp relay ip address

To configure an object group that consists of destination IP addresses to which the packets are forwarded, use the **object-group udp relay ip address** command.

object-group udp relay ip address *object-grp-name*

no object-group udp relay ip address *object-grp-name*

Syntax Description

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

Command Default

None

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 UDP relay feature by using the **ip forward-protocol udp** command. You can create up to 4096 object groups.

Examples

This example shows how to configure the object group:

```
switch# configure terminal
switch(config)# ip forward-protocol udp
switch(config)# object-group udp relay ip address udprelay1
```

This example shows how to delete the the object group:

```
switch(config)# no object-group udp relay ip address udprelay1
```

Related Commands

Command	Description
ip forward-protocol udp	Enables the UDP relay feature.

other-config-flag

To verify the advertised “other” configuration parameter, use the **other-config-flag** command in RA guard policy configuration mode.

other-config-flag {**on**| **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **other-config-flag** command enables verification of the advertised "other" configuration parameter (or "O" flag). This flag could be set by an attacker to force hosts to retrieve other configuration information through a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables O flag verification:

```
switch(config)# ipv6 nd raguard policy raguard1
switch(config-ra-guard)# other-config-flag on
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

P Commands

password secure-mode

To enable secure mode for password changing, use the **password secure-mode** command. To disable the secure mode for password changing, use the **no** form of this command.

password secure-mode

no password secure-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
6.1.4	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable secure mode for changing password:

```
switch# configure terminal
switch(config)# password secure-mode
```

This example shows how to disable secure mode for changing password:

```
switch# configure terminal
switch(config)# no password secure-mode
```

Related Commands

Command	Description
show password strength-check	Enables password-strength checking.

password strength-check

To enable password-strength checking, use the **password strength-check** command. To disable password-strength checking, use the **no** form of this command.

password strength-check

no password strength-check

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

When you enable password-strength checking, the Cisco NX-OS software only allows you to create strong passwords. The characteristics for strong passwords include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

Note When you enable password-strength checking, the Cisco NX-OS software does not check the strength of existing passwords.

This command does not require a license.

Examples

This example shows how to enable password-strength checking:

```
switch# configure terminal
 switch(config)# password strength-check
```

This example shows how to disable password-strength checking:

```
switch# configure terminal
switch(config)# no password strength-check
```

Related Commands

Command	Description
show password strength-check	Enables password-strength checking.
show running-config security	Displays security feature configuration in the running configuration.

periodic

To specify a time range that is active one or more times per week, use the **periodic** command. To remove a periodic time range, use the **no** form of this command.

[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*

no {*sequence-number*| **periodic** *weekday time* **to** [*weekday*] *time*}

[*sequence-number*] **periodic** *list-of-weekdays time* **to** *time*

no {*sequence-number*| **periodic** *list-of-weekdays time* **to** *time*}

Syntax Description

sequence-number	(Optional) Sequence number of the rule, which causes the device to insert the command in that numbered position in the time range. Sequence numbers maintain the order of rules within a time range. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in a time range has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the time range and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
weekday	Day of the week that the range begins or ends. The first occurrence of this argument is the day that the range starts. The second occurrence is the day that the range ends. If the second occurrence is omitted, the end of the range is on the same day as the start of the range. The following keywords are valid values for the *weekday* argument: • **monday** • **tuesday** • **wednesday** • **thursday** • **friday** • **saturday** • **sunday**

time	Time of day that the range starts or ends. The first occurrence of this argument is the time that the range begins. The second occurrence of this argument is the time that the range ends. You can specify the *time* argument in 24-hour notation, in the format *hours*:*minutes* or *hours*:*minutes*:*seconds*. For example, 8:00 a.m. is 8:00 and 8:00 p.m. is 20:00.
to	Separates the first and second occurrences of the *time* argument.
list-of-weekdays	(Optional) Days that the range is in effect. Valid values of this argument are as follows: • A space-delimited list of weekdays, such as the following: `monday thursday friday` • **daily—**All days of the week. • **weekdays—**Monday through Friday. • **weekend—**Saturday through Sunday.

Command Default

to

Command Modes

Time-range 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 a time range named weekend-remote-access-times and configure a periodic rule that allows traffic between 4:00 a.m. and 10:00 p.m. on Saturday and Sunday:

```
switch# configure terminal
switch(config)# time-range weekend-remote-access-times
switch(config-time-range)# periodic weekend 04:00:00 to 22:00:00
```

This example shows how to create a time range named mwf-evening and configure a periodic rule that allows traffic between 6:00 p.m. and 10:00 p.m. on Monday, Wednesday, and Friday:

```
switch# configure terminal
switch(config)# time-range mwf-evening
switch(config-time-range)# periodic monday wednesday friday 18:00:00 to 22:00:00
```

Related Commands

Command	Description
absolute	Configures an absolute time-range rule.
time-range	Configures a time range that you can use in IPv4 and IPv6 ACLs.

permit (ACL)

To enable a capture session for the access control entries (ACEs) of the access control list, use the permit command.

permit protocol {**"0-255"**| **ahp**| **eigrp**| **esp**| **gre**| **icmp**| **igmp**| **ip**| **nos**| **ospf**| **pcp**| **pim**| **tcp**| **udp**}| {**source**| **addrgroup**| **any**| **host**}| {**destination**| **addrgroup**| **any**| **eq**| **gt**| **host**| **lt**| **neq**| **portgroup**| **range**} **capture session** *session*

Syntax Description

0-255	(Optional) Specifies a protocol number.
ahp	(Optional) Specifies Authentication Header Protocol.
eigrp	(Optional) Specifies Cisco's EIGRP routing protocol.
esp	(Optional) Specifies encapsulation security payload.
gre	(Optional) Specifies Cisco's GRE tunneling.
icmp	(Optional) Specifies Internet Control Message Protocol.
igmp	(Optional) Specifies Internet Group Management Protocol.
ip	(Optional) Specifies any IP protocol.
nos	(Optional) Specifies KA9Q NOS compatible IP over IP tunneling.
ospf	(Optional) Specifies OSPF routing protocol.
pcp	(Optional) Specifies Payload Compression Protocol.
pim	(Optional) Specifies protocol independent multicast.
tcp	Specifies Transport Control Protocol.
udp	(Optional) Specifies User Datagram Protocol.
source	Source network address.
addrgroup	(Optional) Specifies the source address group.
any	(Optional) Specifies any source address.
host	(Optional) Specifies a single destination host.

destination	Destination network address.
eq	(Optional) Matches only packets on a given port number.
gt	(Optional) Matches only packets with a greater port number.
lt	(Optional) Matches only packets with a lower port number.
neq	(Optional) Matches only packets not on a given port number.
portgroup	(Optional) Specifies the source port group.
range	(Optional) Matches only packets in the range of port numbers.
capture session	Specifies a capture session for the ACEs.
session	Session ID. The range is from 1 to 48.

Command Default

None

Command Modes

ACL configuration mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable a capture session for the access control entries (ACEs) of the access control list:

```
switch# configure terminal
switch(config)# ip access-list acl-1
switch(config-acl)# permit tcp host 10.1.1.1 any capture session 10
switch(config-acl)#
```

Related Commands

Command	Description
ip access-group *name* **in**	Applies an ACL with capture session ACEs to the interface.
ip access-list	Creates an access list.

permit (ARP)

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

General Syntax

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

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

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

no *sequence-number*

no permit ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

no permit request ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} **[log]**

no permit response ip {**any**| **host** *sender-IP*| *sender-IP sender-IP-mask*} {**any**| **host** *target-IP*| *target-IP target-IP-mask*} **mac** {**any**| **host** *sender-MAC*| *sender-MAC sender-MAC-mask*} [**any**| **host** *target-MAC*| *target-MAC target-MAC-mask*] **[log]**

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.
ip	Introduces the IP address portion of the rule.
any	Specifies that any host matches the part of the rule that contains the **any** keyword. You can use **any** to specify the sender IP address, target IP address, sender MAC address, and target MAC address.

host *sender-IP*	Specifies that the rules matches ARP packets only when the sender IP address in the packet matches the value of the *sender-IP* argument. Valid values for the *sender-IP* argument are IPv4 addresses in dotted-decimal format.
sender-IP sender-IP-mask	IPv4 address and mask for the set of IPv4 addresses that the sender IP address in the packet can match. The *sender-IP* and *sender-IP-mask* argument must be in dotted-decimal format. Specifying 255.255.255.255 as the *sender-IP-mask* argument is the equivalent of using the **host** keyword.
mac	Introduces the MAC address portion of the rule.
host *sender-MAC*	Specifies that the rule matches ARP packets only when the sender MAC address in the packet matches the value of the *sender-MAC* argument. Valid values for the *sender-MAC* argument are MAC addresses in dotted-hexadecimal format.
sender-MAC sender-MAC-mask	MAC address and mask for the set of MAC addresses that the sender MAC address in the packet can match. The *sender-MAC* and *sender-MAC-mask* argument must be in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the *sender-MAC-mask* argument is the equivalent of using the **host** keyword.
log	(Optional) Specifies that the device logs ARP packets that match the rule.
request	(Optional) Specifies that the rule applies only to packets containing ARP request messages. **Note** If you omit both the **request** and the **response** keywords, the rule applies to all ARP messages.
response	(Optional) Specifies that the rule applies only to packets containing ARP response messages. **Note** If you omit both the **request** and the **response** keywords, the rule applies to all ARP messages.
host *target-IP*	Specifies that the rule matches ARP packets only when the target IP address in the packet matches the value of the *target-IP* argument. You can specify **host** *target-IP* only when you use the **response** keyword. Valid values for the *target-IP* argument are IPv4 addresses in dotted-decimal format.

target-IP target-IP-mask	IPv4 address and mask for the set of IPv4 addresses that the target IP address in the packet can match. You can specify *target-IP target-IP-mask* only when you use the **response** keyword. The *target-IP* and *target-IP-mask* argument must be in dotted-decimal format. Specifying 255.255.255.255 as the *target-IP-mask* argument is the equivalent of using the **host** keyword.
host *target-MAC*	Specifies that the rule matches ARP packets only when the target MAC address in the packet matches the value of the *target-MAC* argument. You can specify **host** *target-MAC* only when you use the **response** keyword. Valid values for the *target-MAC* argument are MAC addresses in dotted-hexadecimal format.
target-MAC target-MAC-mask	MAC address and mask for the set of MAC addresses that the target MAC address in the packet can match. You can specify *target-MAC target-MAC-mask* only when you use the **response** keyword. The *target-MAC* and *target-MAC-mask* argument must be in dotted-hexadecimal format. Specifying ffff.ffff.ffff as the *target-MAC-mask* argument is the equivalent of using the **host** keyword.

Command Default

ip

Command Modes

ARP ACL configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A newly created ARP ACL contains no rules.

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

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

If you do not specify either the **response** or **request** keyword, the rule applies to packets that contain any ARP message.

This command does not require a license.

Examples

This example shows how to enter ARP access list configuration mode for an ARP ACL named arp-acl-01 and add a rule that permits ARP request messages that contain a sender IP address that is within the 10.32.143.0 subnet:

```
switch# configure terminal
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)# permit request ip 10.32.143.0 255.255.255.0 mac any
```

Related Commands

Command	Description
deny (ARP)	Configures a deny rule in an ARP ACL.
arp access-list	Configures an ARP ACL.
ip arp inspection filter	Applies an ARP ACL to a VLAN.
remark	Configures a remark in an ACL.
show arp access-list	Displays all ARP ACLs or one ARP ACL.

permit (IPv4)

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

General Syntax

[*sequence-number*] **permit** *protocol source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no permit *protocol source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*| *icmp-type* [*icmp-code*]] [**dscp** *dscp*| **precedence** *precedence*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Group Management Protocol

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] [**dscp** *dscp*| **precedence** *precedence*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Protocol v4

[*sequence-number*] **permit ip** *source destination* [**dscp** *dscp*| **precedence** *precedence*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Transmission Control Protocol

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

User Datagram Protocol

[*sequence-number*] **permit udp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*| **precedence** *precedence*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Syntax Description

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

dscp *dscp*	

(Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords:

- 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010.
- **af11—**Assured Forwarding (AF) class 1, low drop probability (001010)
- **af12—**AF class 1, medium drop probability (001100)
- **af13—**AF class 1, high drop probability (001110)
- **af21—**AF class 2, low drop probability (010010)
- **af22—**AF class 2, medium drop probability (010100)
- **af23—**AF class 2, high drop probability (010110)
- **af31—**AF class 3, low drop probability (011010)
- **af32—**AF class 3, medium drop probability (011100)
- **af33—**AF class 3, high drop probability (011110)
- **af41—**AF class 4, low drop probability (100010)
- **af42—**AF class 4, medium drop probability (100100)
- **af43—**AF class 4, high drop probability (100110)
- **cs1—**Class-selector (CS) 1, precedence 1 (001000)
- **cs2—**CS2, precedence 2 (010000)
- **cs3—**CS3, precedence 3 (011000)
- **cs4—**CS4, precedence 4 (100000)
- **cs5—**CS5, precedence 5 (101000)
- **cs6—**CS6, precedence 6 (110000)

	• **cs7—**CS7, precedence 7 (111000) • **default—**Default DSCP value (000000) • **ef—**Expedited Forwarding (101110)
precedence *precedence*	(Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword, as follows: • 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011. • **critical—**Precedence 5 (101) • **flash—**Precedence 3 (011) • **flash-override—**Precedence 4 (100) • **immediate—**Precedence 2 (010) • **internet—**Precedence 6 (110) • **network—**Precedence 7 (111) • **priority—**Precedence 1 (001) • **routine—**Precedence 0 (000)
fragments	(Optional) Specifies that the rule matches only those packets that are noninitial fragments. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: • Whether the protocol was TCP, UDP, ICMP or a number protocol • Source and destination addresses • Source and destination port numbers, if applicable

time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. Use the **time-range** command to a time range.
icmp-message	(ICMP only: Optional) ICMP message that the rule matches. This argument can be one of the keywords listed under "ICMP Message Types" in the "Usage Guidelines" section.
icmp-type [*icmp-code*]	(ICMP only: Optional) ICMP message type that the rule matches. Valid values for the *icmp-type* argument are an integer from 0 to 255. If the ICMP message type supports message codes, you can use the *icmp-code* argument to specify the code that the rule matches. For more information about ICMP message types and codes, see http://www.iana.org/assignments/icmp-parameters .
igmp-message	(IGMP only: Optional) IGMP message type that the rule matches. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords: • **dvmrp—**Distance Vector Multicast Routing Protocol • **host-query—**Host query • **host-report—**Host report • **pim—**Protocol Independent Multicast • **trace—**Multicast trace

operator port [*port*]	(Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the port in the packet is equal to the *port* argument. • **gt—**Matches only if the port in the packet is greater than and not equal to the *port* argument. • **lt—**Matches only if the port in the packet is less than and not equal to the *port* argument. • **neq—**Matches only if the port in the packet is not equal to the *port* argument. • **range—**Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.
portgroup *portgroup*	(Optional; TCP and UDP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port object group specified by the *portgroup* argument, which can be up to 64 alphanumeric, case-sensitive characters. Whether the IP port object group applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port object objects.

flags	(TCP only; Optional) TCP control bit flags that the rule matches. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.
packet-length*operatorpacket-length* [*packet-length*	(Optional) Rule matches only packets that have a length in bytes that satisfies the condition specified by the *operator* and *packet-length* arguments. Valid values for the *packet-length* argument are whole numbers from 20 to 9210. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the packet length in bytes is equal to the *packet-length* argument. • **gt—**Matches only if the packet length in bytes is greater than the *packet-length* argument. • **lt—**Matches only if the packet length in bytes is less than the *packet-length* argument. • **neq—**Matches only if the packet length in bytes is not equal to the *packet-length* argument. • **range—**Requires two *packet-length* arguments and matches only if the packet length in bytes is equal to or greater than the first *packet-length* argument and equal to or less than the second *packet-length* argument.

Command Default

A newly created IPv4 ACL contains no rules.

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

Command Modes

IPv4 ACL configuration

Command History

Release	Modification
4.1(2)	Support was added for the following: • The **ahp**, **eigrp**, **esp**, **gre**, **nos**, **ospf**, **pcp**, and **pim** protocol keywords. • The **packet-length** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

When the device applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

This command does not require a license.

Protocol

You can specify the protocol of packets that the rule applies to by the protocol name or the number of the protocol. If you want the rule to apply to all IPv4 traffic, use the **ip** keyword.

The protocol keyword that you specify affects the additional keywords and arguments that are available. Unless otherwise specified, only the other keywords that apply to all IPv4 protocols are available. Those keywords include the following:

-
    - **dscp**
    - **fragments**
    - **log**
    - **packet-length**
    - **precedence**
    - **time-range**

Valid protocol numbers are from 0 to 255.

Valid protocol names are the following keywords:

- **ahp—**Specifies that the rule applies to authentication header protocol (AHP) traffic only.
- **eigrp—**Specifies that the rule applies to Enhanced Interior Gateway Routing Protocol (EIGRP) traffic only.
- **esp—**Specifies that the rule applies to Encapsulating Security Protocol (ESP) traffic only.
- **gre—**Specifies that the rule applies to General Routing Encapsulation (GRE) traffic only.

- **icmp—**Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **igmp—**Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **ip—**Specifies that the rule applies to all IPv4 traffic.
- **nos—**Specifies that the rule applies to KA9Q NOS-compatible IP-over-IP tunneling traffic only.
- **ospf—**Specifies that the rule applies to Open Shortest Path First (OSPF) traffic only.
- **pcp—**Specifies that the rule applies to payload compression protocol (PCP) traffic only.
- **pim—**Specifies that the rule applies to protocol-independent multicast (PIM) traffic only.
- **tcp—**Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **udp—**Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.

Source and Destination

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

- IP address group object—You can use an IPv4 address group object to specify a *source* or *destination* argument. Use the **object-group ip address** command to create and change IPv4 address group objects. The syntax is as follows:

```
addrgroup

address-group-name
```

The following example shows how to use an IPv4 address object group named lab-gateway-svrs to specify the *destination* argument:

```
switch(config-acl)# permit ip any addrgroup lab-gateway-svrs
```

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

```
IPv4-address network-wildcard
```

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

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

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

```
IPv4-address/prefix-len
```

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

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

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

```
host
IPv4-address
```

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

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

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

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

ICMP Message Types

The *icmp-message* argument can be one of the following keywords:

- **administratively-prohibited—**Administratively prohibited
- **alternate-address—**Alternate address
- **conversion-error—**Datagram conversion
- **dod-host-prohibited—**Host prohibited
- **dod-net-prohibited—**Net prohibited
- **echo—**Echo (ping)
- **echo-reply—**Echo reply
- **general-parameter-problem—**Parameter problem
- **host-isolated—**Host isolated
- **host-precedence-unreachable—**Host unreachable for precedence
- **host-redirect—**Host redirect
- **host-tos-redirect—**Host redirect for ToS
- **host-tos-unreachable—**Host unreachable for ToS
- **host-unknown—**Host unknown
- **host-unreachable—**Host unreachable
- **information-reply—**Information replies
- **information-request—**Information requests
- **mask-reply—**Mask replies
- **mask-request—**Mask requests
- **mobile-redirect—**Mobile host redirect

- **net-redirect—**Network redirect
- **net-tos-redirect—**Net redirect for ToS
- **net-tos-unreachable—**Network unreachable for ToS
- **net-unreachable—**Net unreachable
- **network-unknown—**Network unknown
- **no-room-for-option—**Parameter required but no room
- **option-missing—**Parameter required but not present
- **packet-too-big—**Fragmentation needed and DF set
- **parameter-problem—**All parameter problems
- **port-unreachable—**Port unreachable
- **precedence-unreachable—**Precedence cutoff
- **protocol-unreachable—**Protocol unreachable
- **reassembly-timeout—**Reassembly timeout
- **redirect—**All redirects
- **router-advertisement—**Router discovery advertisements
- **router-solicitation—**Router discovery solicitations
- **source-quench—**Source quenches
- **source-route-failed—**Source route failed
- **time-exceeded—**All time exceeded messages
- **timestamp-reply—**Timestamp replies
- **timestamp-request—**Timestamp requests
- **traceroute—**Traceroute
- **ttl-exceeded—**TTL exceeded
- **unreachable—**All unreachables

TCP Port Names

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

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—Exec (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (20)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—UNIX-to-UNIX Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 80)

UDP Port Names

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

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

non500-isakmp—Internet Security Association and Key Management Protocol (45)

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

xdmcp—X Display Manager Control Protocol (177)

Examples

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

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

This example shows how to configure an IPv4 ACL named acl-eng-to-marketing with a rule that permits all IP traffic from an IP-address object group named eng_workstations to an IP-address object group named marketing_group:

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

Related Commands

Command	Description
deny (IPv4)	Configures a deny rule in an IPv4 ACL.

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ip access-list	Configures an IPv4 ACL.
object-group ip address	Configures an IPv4 address object group.
object-group ip port	Configures an IP port object group.
remark	Configures a remark in an ACL.
show ip access-list	Displays all IPv4 ACLs or one IPv4 ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
time-range	Configures a time range.

permit (IPv6)

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

General Syntax

[*sequence-number*] **permit** *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no permit *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no *sequence-number*

Internet Control Message Protocol

[*sequence-number*| **no**] **permit icmp** *source destination* [*icmp-message*| *icmp-type* [*icmp-code*]] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Internet Protocol v6

[*sequence-number*] **permit ipv6** *source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Stream Control Transmission Protocol

[*sequence-number*| **no**] **permit sctp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Transmission Control Protocol

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

User Datagram Protocol

[*sequence-number*| **no**] **permit udp** *source* [*operator port* [*port*]| **portgroup** *portgroup*] *destination* [*operator port* [*port*]| **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] **[fragments]** **[log]** [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Syntax Description

sequence-number	(Optional) Sequence number of the **permit** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to rules.

protocol	

Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords:

- **ahp—**Specifies that the rule applies to Authentication Header Protocol (AHP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **esp—**Specifies that the rule applies to Encapsulating Security Payload (ESP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **icmp—**Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **ipv6—**Specifies that the rule applies to all IPv6 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **pcp—**Specifies that the rule applies to Payload Compression Protocol (PCP) traffic only. When you use this keyword, only the other keywords and arguments that apply to all IPv6 protocols are available.
- **sctp—**Specifies that the rule applies to Stream Control Transmission Protocol (SCTP) traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **tcp—**Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument.
- **udp—**Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol*

	argument.
source	Source IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.
destination	Destination IPv6 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section.

dscp *dscp*	

(Optional) Specifies that the rule matches only packets with the specified 6-bit differentiated services value in the DSCP field of the IPv6 header. The *dscp* argument can be one of the following numbers or keywords:

- 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only packets that have the following bits in the DSCP field: 001010.
- **af11**—Assured Forwarding (AF) class 1, low drop probability (001010)
- **af12**—AF class 1, medium drop probability (001100)
- **af13**—AF class 1, high drop probability (001110)
- **af21**—AF class 2, low drop probability (010010)
- **af22**—AF class 2, medium drop probability (010100)
- **af23**—AF class 2, high drop probability (010110)
- **af31**—AF class 3, low drop probability (011010)
- **af32**—AF class 3, medium drop probability (011100)
- **af33**—AF class 3, high drop probability (011110)
- **af41**—AF class 4, low drop probability (100010)
- **af42**—AF class 4, medium drop probability (100100)
- **af43**—AF class 4, high drop probability (100110)
- **cs1**—Class-selector (CS) 1, precedence 1 (001000)
- **cs2**—CS2, precedence 2 (010000)
- **cs3**—CS3, precedence 3 (011000)
- **cs4**—CS4, precedence 4 (100000)
- **cs5**—CS5, precedence 5 (101000)
- **cs6**—CS6, precedence 6 (110000)

	• **cs7—**CS7, precedence 7 (111000) • **default—**Default DSCP value (000000) • **ef—**Expedited Forwarding (101110)
flow-label *flow-label-value*	(Optional) Specifies that the rule matches only IPv6 packets whose Flow Label header field has the value specified by the *flow-label-value* argument. The *flow-label-value* argument can be an integer from 0 to 1048575.
fragments	(Optional) Specifies that the rule matches noninitial fragmented packets only. The device considers noninitial fragmented packets to be packets with a fragment extension header that contains a fragment offset that is not equal to zero. You cannot specify this keyword in the same rule that you specify Layer 4 options, such as a TCP port number, because the information that the devices requires to evaluate those options is contained only in initial fragments.
log	(Optional) Specifies that the device generates an informational logging message about each packet that matches the rule. The message includes the following information: • Whether the protocol was TCP, UDP, ICMP or a number protocol • Source and destination addresses • Source and destination port numbers, if applicable
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.
icmp-message	(ICMP only: Optional) ICMPv6 message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMPv6 Message Types” in the “Usage Guidelines” section.

icmp-type [*icmp-code*]	(ICMP only: Optional) ICMP message type that the rule matches. Valid values for the *icmp-type* argument are an integer from 0 to 255. If the ICMP message type supports message codes, you can use the *icmp-code* argument to specify the code that the rule matches. For more information about ICMP message types and codes, see http://www.iana.org/assignments/icmp-parameters .
operator port port	(Optional; TCP, UDP, and SCTP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument. The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section. A second *port* argument is required only when the *operator* argument is a range. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the port in the packet is equal to the *port* argument. • **gt—**Matches only if the port in the packet is greater than and not equal to the *port* argument. • **lt—**Matches only if the port in the packet is less than and not equal to the *port* argument. • **neq—**Matches only if the port in the packet is not equal to the *port* argument. • **range—**Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument.

portgroup *portgroup*	(Optional; TCP, UDP, and SCTP only) Specifies that the rule matches only packets that are from a source port or to a destination port that is a member of the IP port-group object specified by the *portgroup* argument. Whether the port-group object applies to a source port or a destination port depends upon whether you specify it after the *source* argument or after the *destination* argument. Use the **object-group ip port** command to create and change IP port-group objects.
established	(TCP only; Optional) Specifies that the rule matches only packets that belong to an established TCP connection. The device considers TCP packets with the ACK or RST bits set to belong to an established connection.
flags	(TCP only; Optional) Rule matches only packets that have specific TCP control bit flags set. The value of the *flags* argument must be one or more of the following keywords: • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**

packet-length*operatorpacket-length* [*packet-length*	(Optional) Rule matches only packets that have a length in bytes that satisfies the condition specified by the *operator* and *packet-length* arguments. Valid values for the *packet-length* argument are whole numbers from 20 to 9210. The *operator* argument must be one of the following keywords: • **eq—**Matches only if the packet length in bytes is equal to the *packet-length* argument. • **gt—**Matches only if the packet length in bytes is greater than the *packet-length* argument. • **lt—**Matches only if the packet length in bytes is less than the *packet-length* argument. • **neq—**Matches only if the packet length in bytes is not equal to the *packet-length* argument. • **range—**Requires two *packet-length* arguments and matches only if the packet length in bytes is equal to or greater than the first *packet-length* argument and equal to or less than the second *packet-length* argument.

Command Default

None

Command Modes

IPv6 ACL configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

A newly created IPv6 ACL contains no rules.

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

This command does not require a license.

Source and Destination

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

- IPv6 address group object—You can use an IPv6 address group object to specify a *source* or *destination* argument. Use the **object-group ipv6 address** command to create and change IPv6 address group objects. The syntax is as follows:

```
addrgroup

address-group-name
```

The following example shows how to use an IPv6 address object group named lab-svrs-1301 to specify the *destination* argument:

```
switch(config-acl)# permit ipv6 any addrgroup lab-svrs-1301
```

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

```
IPv6-address/prefix-len
```

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

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

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

```
host
IPv6-address
```

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

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

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

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

ICMPv6 Message Types

The *icmp-message* argument can be one of the following keywords:

- **beyond-scope—**Destination beyond scope
- **destination-unreachable—**Destination address is unreachable
- **echo-reply—**Echo reply
- **echo-request—**Echo request (ping)
- **header—**Parameter header problems
- **hop-limit—**Hop limit exceeded in transit
- **mld-query—**Multicast Listener Discovery Query
- **mld-reduction—**Multicast Listener Discovery Reduction
- **mld-report—**Multicast Listener Discovery Report
- **nd-na—**Neighbor discovery neighbor advertisements
- **nd-ns—**Neighbor discovery neighbor solicitations

- **next-header—**Parameter next header problems
- **no-admin—**Administration prohibited destination
- **no-route—**No route to destination
- **packet-too-big—**Packet too big
- **parameter-option—**Parameter option problems
- **parameter-problem—**All parameter problems
- **port-unreachable—**Port unreachable
- **reassembly-timeout—**Reassembly timeout
- **redirect—**Neighbor redirect
- **renum-command—**Router renumbering command
- **renum-result—**Router renumbering result
- **renum-seq-number—**Router renumbering sequence number reset
- **router-advertisement—**Neighbor discovery router advertisements
- **router-renumbering—**All router renumbering
- **router-solicitation—**Neighbor discovery router solicitations
- **time-exceeded—**All time exceeded messages
- **unreachable—**All unreachable

TCP Port Names

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

bgp—Border Gateway Protocol (179)

chargen—Character generator (19)

cmd—Remote commands (rcmd, 514)

daytime—Daytime (13)

discard—Discard (9)

domain—Domain Name Service (53)

drip—Dynamic Routing Information Protocol (3949)

echo—Echo (7)

exec—Exec (rsh, 512)

finger—Finger (79)

ftp—File Transfer Protocol (21)

ftp-data—FTP data connections (20)

gopher—Gopher (7)

hostname—NIC hostname server (11)

ident—Ident Protocol (113)

irc—Internet Relay Chat (194)

klogin—Kerberos login (543)

kshell—Kerberos shell (544)

login—Login (rlogin, 513)

lpd—Printer service (515)

nntp—Network News Transport Protocol (119)

pim-auto-rp—PIM Auto-RP (496)

pop2—Post Office Protocol v2 (19)

pop3—Post Office Protocol v3 (11)

smtp—Simple Mail Transport Protocol (25)

sunrpc—Sun Remote Procedure Call (111)

tacacs—TAC Access Control System (49)

talk—Talk (517)

telnet—Telnet (23)

time—Time (37)

uucp—Unix-to-Unix Copy Program (54)

whois—WHOIS/NICNAME (43)

www—World Wide Web (HTTP, 80)

UDP Port Names

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

biff—Biff (mail notification, comsat, 512)

bootpc—Bootstrap Protocol (BOOTP) client (68)

bootps—Bootstrap Protocol (BOOTP) server (67)

discard—Discard (9)

dnsix—DNSIX security protocol auditing (195)

domain—Domain Name Service (DNS, 53)

echo—Echo (7)

isakmp—Internet Security Association and Key Management Protocol (5)

mobile-ip—Mobile IP registration (434)

nameserver—IEN116 name service (obsolete, 42)

netbios-dgm—NetBIOS datagram service (138)

netbios-ns—NetBIOS name service (137)

netbios-ss—NetBIOS session service (139)

non500-isakmp—Internet Security Association and Key Management Protocol (45)

ntp—Network Time Protocol (123)

pim-auto-rp—PIM Auto-RP (496)

rip—Routing Information Protocol (router, in.routed, 52)

snmp—Simple Network Management Protocol (161)

snmptrap—SNMP Traps (162)

sunrpc—Sun Remote Procedure Call (111)

syslog—System Logger (514)

tacacs—TAC Access Control System (49)

talk—Talk (517)

tftp—Trivial File Transfer Protocol (69)

time—Time (37)

who—Who service (rwho, 513)

xdmcp—X Display Manager Control Protocol (177)

Examples

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

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

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

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

Related Commands

Command	Description
deny (IPv6)	Configures a deny rule in an IPv6 ACL.
fragments	Configures how an IP ACL processes noninitial fragments.
ipv6 access-list	Configures an IPv6 ACL.
object-group ipv6 address	Configures an IPv6-address object group.
object-group ip port	Configures an IP-port object group.
remark	Configures a remark in an ACL.
show ipv6 access-list	Displays all IPv6 ACLs or one IPv6 ACL.

Command	Description
statistics per-entry	Enables collection of statistics for each entry in an ACL.
time-range	Configures a time range.

permit (MAC)

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

[*sequence-number*] **permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*] [**time-range** *time-range-name*]

no permit *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*] [**time-range** *time-range-name*]

no *sequence-number*

Syntax Description

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

vlan *VLAN-ID*	(Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the VLAN ID given. The *VLAN-ID* argument can be an integer from 1 to 4094.
time-range *time-range-name*	(Optional) Specifies the time range that applies to this rule. You can configure a time range by using the **time-range** command.

Command Default

None

Command Modes

MAC ACL configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

A newly created MAC ACL contains no rules.

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

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

This command does not require a license.

Source and Destination

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

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

```
MAC-address MAC-mask
```

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

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

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

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

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

MAC Protocols

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

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

Examples

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

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

Related Commands

Command	Description
deny (MAC)	Configures a deny rule in a MAC ACL.
mac access-list	Configures a MAC ACL.
remark	Configures a remark in an ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
show mac access-list	Displays all MAC ACLs or one MAC ACL.
time-range	Configures a time range.

permit (role-based access control list)

To configure a permit action in a security group access control list (SGACL), use the **permit** command. To remove the action, use the **no** form of this command.

permit {**all**| **icmp**| **igmp**| **ip**| {**tcp**| **udp**} [{**src**| **dst**} {**eq**| **gt**| **lt**| **neq**} *port-number*| **range** *port-number1* *port-number2*]} **[log]**

nopermit {**all**| **icmp**| **igmp**| **ip**| {**tcp**| **udp**} [{**src**| **dst**} {**eq**| **gt**| **lt**| **neq**} *port-number*| **range** *port-number1* *port-number2*]} **[log]**

Syntax Description

all	Specifies all traffic.
icmp	Specifies Internet Control Message Protocol (ICMP) traffic.
igmp	Specifies Internet Group Management Protocol (IGMP) traffic.
ip	Specifies IP traffic.
tcp	Specifies TCP traffic.
udp	Specifies User Datagram Protocol (UDP) traffic.
src	Specifies the source port number.
dst	Specifies the destination port number
eq	Specifies equal to the port number.
gt	Specifies greater than the port number.
lt	Specifies less than the port number.
neq	Specifies not equal to the port number.
port-number	Port number for TCP or UDP. The range is from 0 to 65535.
range	Specifies a port range for TCP or UDP.
port-number1	First port in the range. The range is from 0 to 65535.
port-number2	Last port in the range. The range is from 0 to 65535.
log	(Optional) Specifies that packets matching this configuration be logged.

Command Default

None

Command Modes

role-based access control list

Command History

Release	Modification
5.0(2)	The **log** keyword was added to support the enabling of role-based access control list (RBACL) logging.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

To enable RBACL logging, you must enable RBACL policy enforcement on the VLAN and VRF.

To enable RBACL logging, you must set the logging level of ACLLOG syslogs to 6 and the logging level of CTS manager syslogs to 5.

This command requires the Advanced Services license.

Examples

This example shows how to add a permit action to an SGACL and enable RBACL logging:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# permit icmp log
```

This example shows how to remove a permit action from an SGACL:

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no permit icmp log
```

Related Commands

Command	Description
cts role-based access-list	Configures Cisco TrustSec SGACLs.
deny (role-based access control list)	Configures deny actions in an SGACL.
feature cts	Enables the Cisco TrustSec feature.
show cts role-based access-list	Displays the Cisco TrustSec SGACL configuration.

permit interface

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

permit interface {**ethernet** *slot* / *port [-port2]*| *interface-list*}

no permit interface

Syntax Description

ethernet *slot*/*port*	Specifies the Ethernet interface identifier.
-*port*	Last interface in a range of interfaces on a module.
interface-list	Comma-separated list of Ethernet interface identifiers.

Command Default

All interfaces

Command Modes

User role interface policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **interface policy deny** command denies a user role access to all interfaces except for those that you allow with the **permit interface** command.

This command does not require a license.

Examples

This example shows how to permit a range of interfaces for a user role interface policy:

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

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

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5,
ethernet 1/7
```

This example shows how to deny an interface in a user role interface policy:

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

Related Commands

Command	Description
interface policy deny	Enters interface policy configuration mode for a user role.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

permit vlan

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

permit vlan {*vlan-id [-vlan-id2]*| *vlan-list*}

no permit vlan

Syntax Description

vlan-id	VLAN identifier. The range is 1-3967 and 4048-4093.
- vlan-id2	Last VLAN identifier in a range. The VLAN identifier must be greater than the first VLAN identifier in the range.
vlan-list	Comma-separated list of VLAN identifiers.

Command Default

All VLANs

Command Modes

User role VLAN policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **vlan policy deny** command denies a user role access to all VLANs except for those that you allow with the **permit vlan** command.

This command does not require a license.

Examples

This example shows how to permit a VLAN identifier for a user role VLAN policy:

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

This example shows how to permit a range of VLAN identifiers for a user role VLAN policy:

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

This example shows how to permit a list of VLAN identifiers for a user role VLAN policy:

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

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

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

Related Commands

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

permit vrf

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

permit vrf *vrf-name*

no permit vrf *vrf-name*

Syntax Description

vrf-name	VRF name. The name is case sensitive.

Command Default

All VRFs

Command Modes

User role VRF policy configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **vrf policy deny** command denies a user role access to all VRFs except for those that you allow with the **permit vrf** command.

You can repeat this command to allow more than on VRF name for the user role.

This command does not require a license.

Examples

This example shows how to permit a VRF name for a user role VRF policy:

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

This example shows how to permit a VRF name from a user role VRF policy:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# no permit vrf engineering
```

Related Commands

Command	Description
vrf policy deny	Enters VRF policy configuration mode for a user role.

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

platform access-list update

To configure how supervisor modules update I/O modules with changes to access control lists (ACLs), use the **platform access-list update** command. To disable atomic updates, use the **no** form of this command.

platform access-list update {**atomic**| **default-result permit**}

no platform access-list update {**atomic**| **default-result permit**}

Syntax Description

atomic	Specifies that the device performs atomic updates, which do not disrupt traffic during the update. By default, a Cisco NX-OS device performs atomic ACL updates.
default-result permit	Specifies that, during non-atomic updates, the device permits traffic that the updated ACL applies to.

Command Default

atomic

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was deprecated and replace with the **access-list update** command.
4.0(1)	This command was introduced.

Usage Guidelines

By default, a Cisco NX-OS device performs atomic ACL updates, which do not disrupt traffic that the updated ACL applies to; however, atomic updates require that the I/O modules that receive the updates have enough available resources to store each of the updated entries in the affected ACL. After the update occurs, the additional resources used for the update are freed. If the I/O module lacks the required resources, the device generates an error message and the ACL update to the I/O module fails.

If an I/O module lacks required resources, you can disable atomic updates by using the **no platform access-list update atomic** command; however, during the brief time required for the device to remove the old ACL and implement the updated ACL, traffic that the ACL applies to is dropped by default.

If you want to permit all traffic that the updated ACL applies during a non-atomic update, use the **platform access-list update default-result permit** command.

This command does not require a license.

Examples

This example shows how disable atomic updates to ACLs:

```
switch# configure terminal
switch(config)# no platform access-list update atomic
```

This example shows how to permit affected traffic during a non-atomic ACL update:

```
switch# configure terminal
switch(config)# platform access-list update default-result permit
```

This example shows how to revert to the atomic update method:

```
switch# configure terminal
switch(config)# no platform access-list update default-result permit
switch(config)# platform access-list update atomic
```

Related Commands

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

platform rate-limit

To configure rate limits in packets per second on supervisor-bound traffic, use the **platform rate-limit** command. To revert to the default, use the **no** form of this command.

platform rate-limit {**access-list-log**| **copy**| **layer-2** {**port-security**| **storm-control**}| **layer-3** {**control**| **glean**| **mtu**| **multicast** {**directly-connect**| **local-groups**| **rpf-leak**}| **ttl**}| **receive**} *packets*

no platform rate-limit {**access-list-log**| **copy**| **layer-2** {**port-security**| **storm-control**}| **layer-3** {**control**| **glean**| **mtu**| **multicast** {**directly-connect**| **local-groups**| **rpf-leak**}| **ttl**}| **receive**} [*packets*]

Syntax Description

access-list-log	Specifies packets copied to the supervisor module for access list logging. The default rate is 100 packets per second.
copy	Specifies data and control packets copied to the supervisor module. The default rate is 30000 packets per second.
layer-2	Specifies Layer 2 packets rate limits.
port-security	Specifies port security packets. The default is disabled.
storm-control	Specifies storm control packets. The default is disabled.
layer-3	Specifies Layer 3 packets.
control	Specifies Layer-3 control packets. The default rate is 10000 packets per second.
glean	Specifies Layer-3 glean packets. The default rate is 100 packets per second.
mtu	Specifies Layer-3 MTU failure redirected packets. The default rate is 500 packets per second.
multicast	Specifies Layer-3 multicast packets per second.
directly-connect	Specifies directly connected multicast packets. The default rate is 10000 packets per second.
local-groups	Specifies local groups multicast packets. The default rate is 10000 packets per second.
rpf-leak	Specifies Reverse Path Forwarding (RPF) leak packets. The default rate is 500 packets per second.

ttl	Specifies Layer-3 failed time-to-live redirected packets. The default rate is 500 packets per second.
receive	Specifies packets redirected to the supervisor module. The default rate is 30000 packets per second.
packets	Number of packets per second. The range is from 1 to 33554431.

Command Default

See Syntax Description for the default rate limits.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was deprecated and replaced with the **rate-limiter** command.
4.0(3)	Added the **port-security** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a rate limit for control packets:

```
switch# configure terminal
switch(config)# platform rate-limit layer-3 control 20000
```

This example shows how to revert to the default rate limit for control packets:

```
switch# configure terminal
switch(config)# no platform rate-limit layer-3 control
```

Related Commands

Command	Description
show running-config	Displays the running configuration.

police (policy map)

To configure policing for a class map in a control plane policy map, use the **police** command. To remove policing for a class map in a control plane policy map, use the **no** form of this command.

police [cir] *cir-rate* [**bps| gbps| kbps| mbps| pps**]

police [cir] *cir-rate* [**bps| gbps| kbps| mbps**] **[bc]** *burst-size* [**bytes| kbytes| mbytes| ms| packets| us**]

police [cir] *cir-rate* [**bps| gbps| kbps| mbps| pps**] **conform** {**drop| set-cos-transmit** *cos-value*| **set-dscp-transmit** *dscp-value*| **set-prec-transmit** *prec-valu* **e| transmit**} [**exceed** {**drop| set dscp dscp table cir-markdown-map| transmit**}] [**violate** {**drop| set dscp dscp table pir-markdown-map| transmit**}]

police [cir] *cir-rate* [**bps| gbps| kbps| mbps| pps**] **pir** *pir-rate* [**bps| gbps| kbps| mbps**] [**[be]** *extended-burst-size* [**bytes| kbytes| mbytes| ms| packets| us**]]

no police [cir] *cir-rate* [**bps| gbps| kbps| mbps| pps**]

no police [cir] *cir-rate* [**bps| gbps| kbps| mbps| pps**] **[bc]** *burst-size* [**bytes| kbytes| mbytes| ms| packets| us**]

no police [cir] *cir-rate* [**bps| gbps| kbps| mbps| pps**] **conform** {**drop| set-cos-transmit** *cos-value*| **set-dscp-transmit** *dscp-value*| **set-prec-transmit** *prec-valu* **e| transmit**} [**exceed** {**drop| set dscp dscp table cir-markdown-map| transmit**}] [**violate** {**drop| set dscp dscp table pir-markdown-map| transmit**}]

no police [cir] *cir-rate* [**bps| gbps| kbps| mbps| pps**] **pir** *pir-rate* [**bps| gbps| kbps| mbps| pps**] [**[be]** *extended-burst-size* [**bytes| kbytes| mbytes| ms| packets| us**]]

Syntax Description

cir	(Optional) Specifies the committed information rate (CIR).
cir-rate	CIR rate. The range is from 0 to 80000000000.
bps	(Optional) Specifies units for traffic rates bytes per second in bits per second.
gbps	(Optional) Specifies units for traffic rates in gigabits per second.
kbps	(Optional) Specifies units for traffic rates in kilobits per second.
mbps	(Optional) Specifies units for traffic rates in megabits per second.
pps	(Optional) Specifies units for traffic rates in packets per second.
bc	(Optional) Specifies the committed burst size.
burst-size	Committed burst size. The range is from 1 to 512000000.

bytes	(Optional) Specifies the units for a burst in bytes.
kbytes	(Optional) Specifies the units for a burst in kilobytes.
mbytes	(Optional) Specifies the units for a burst in megabytes.
ms	(Optional) Specifies the units for a burst in milliseconds.
packets	(Optional) Specifies the units for a burst in packets.
us	(Optional) Specifies the units for a burst in microseconds.
conform	Configures an action when the traffic conforms to the specified rates and bursts.
drop	Specifies the drop action.
set-cos-transmit *cos-value*	Specifies setting the class of service (CoS) value. The range is from 0 to 7.
set-dscp-transmit *dscp-value*	Specifies the differentiated services code point (DSCP) value for IPv4 and IPv6 packets. The range is from 0 to 63.
set-prec-transmit *prec-value*	Specifies the precedence value for IPv4 and IPv6 packets. The range is from 0 to 7.
transmit	Specifies the transmit action.
exceed	Configures an action when the traffic exceeds the specified rates and bursts.
set dscp dscp table cir-markdown-map	Flags the packet on the CIR markdown map.
violate	(Optional) Configures an action when the traffic violates the specified rates and bursts.
set dscp dscp table pir-markdown-map	Flags the packet on the PIR markdown map.
pir *pir-rate*	Specifies the PIR rate.
be	(Optional) Specifies the extended burst size.
extended-burst-size	Extended burst size. The range is from 1 to 512000000.

Command Default

None

Command Modes

Policy map configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default VDC.

This command does not require a license.

Examples

This example shows how to specify a control plane policy map and enter policy map configuration mode:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# police cir 2000 kbps
```

This example shows how to delete a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no police 2000 kbps
```

Related Commands

Command	Description
class (policy map)	Specifies a control plane class map for a control plane policy map and enters policy map class configuration mode.
show policy-map type control-plane	Displays configuration information for control plane policy maps.

policy

To manually configure a Cisco TrustSec authentication policy on an interface with either a Cisco TrustSec device identifier or security group tag (SGT), use the **policy** command. To revert to the default, use the **no** form of this command.

policy {**dynamic identity** *device-id*| **static sgt** *sgt-value* **[trusted]**}

no policy {**dynamic**| **static**}

Syntax Description

dynamic identity	Specifies a dynamic policy using a Cisco TrustSec device identifier.
device-id	Cisco TrustSec device identifier. The device identifier is case sensitive.
static sgt	Specifies a static policy using an SGT.
sgt-value	Cisco TrustSec SGT. The sgt-value is either a decimal value or a hexadecimal value in the format 0xhhhh. The decimal range is from 2 to 65519, and the hexadecimal range is from 0x2 to 0xffef.
trusted	(Optional) Specifies that the traffic coming on the interface with the SGT should not have its tag overridden.

Command Default

None

Command Modes

Cisco TrustSec manual configuration

Command History

Release	Modification
6.2(2)	Modified the sgt-value argument to accept decimal values.
4.0(3)	Removed the keywords and options following **dynamic** and **static** in the **no** form of this command.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to manually configure a dynamic Cisco TrustSec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to remove a manually configured dynamic Cisco TrustSec policy from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to manually configure a static Cisco TrustSec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to remove a manually configured static Cisco TrustSec policy on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
cts manual	Enters Cisco TrustSec manual configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

policy-map type control-plane

To create or specify a control plane policy map and enter policy map configuration mode, use the **policy-map type control-plane** command. To delete a control plane policy map, use the **no** form of this command.

policy-map type control-plane *policy-map-name*

no policy-map type control-plane *policy-map-name*

Syntax Description

policy-map-name	Name of the class map. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default VDC.

This command does not require a license.

Examples

This example shows how to specify a control plane policy map and enter policy map configuration mode:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)#
```

This example shows how to delete a control plane policy map:

```
switch# configure terminal
switch(config)# no policy-map type control-plane PolicyMapA
```

Related Commands

Command	Description
show policy-map type control-plane	Displays configuration information for control plane policy maps.

preference

To enable verification that the advertised preference (in preference option) is greater than the minimum specified limit and less than the maximum specified limit, use the **preference** command in Dynamic Host Configuration Protocol version 6 (DHCPv6) guard configuration mode. To remove the preference, use the **no** form of this command.

preference {**max**| **min**}*limit*

Syntax Description

limit	The maximum or minimum limit that the advertised preference must conform to. The acceptable range is from 0 to 255.

Command Default

No preference value is set.

Command Modes

DHCPv6 guard configuration (config-dhcp-guard)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

This command enables verification that the advertised preference is not greater than the maximum specified limit or less than the minimum specified limit.

Examples

The following example defines an DHCPv6 guard policy name as policy1, places the router in DHCPv6 guard configuration mode, and enables verification that the advertised preference is not greater than 254 or less than 2:

```
switch(config)# ipv6 dhcp guard policy policy1
switch(config-dhcp-guard)# preference min 2
switch(config-dhcp-guard)# preference max 254
```

Related Commands

Command	Description
ipv6 dhcp guard policy	Defines the DHCPv6 guard policy name.

propagate-sgt

To enable SGT propagation on Layer 2 (L2) Cisco TrustSec interfaces, use the **propagate-sgt** command. To disable SGT propagation, use the **no** form of this command.

propagate-sgt [l2-control]

no propagate-sgt [l2-control]

Syntax Description

l2-control	Specifies SGT propagation of the L2 control packets.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
8.1(1)	Added the **l2-control** keyword.
6.2(10)	Support was added for F3 Series modules.
4.0(3)	This command was introduced.

Usage Guidelines

You can disable the SGT propagation feature on an interface if the peer device connected to the interface can not handle Cisco TrustSec packets tagged with an SGT.

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

Use the **no propagate-sgt l2-control** command to enable SGT tagging exemption for L2 control packets. This exemption ensures that the L2 control protocols are transmitted without any SGT tags from the Cisco TrustSec enabled-ports. The **no propagate-sgt l2-control** command is supported only on the Cisco M3 Series module ports without Cisco TrustSec MACSec.

You can also enable or disable SGT tagging of the L2 control packets under a port profile and a port channel.

This command requires the Advanced Services license.

Examples

This example shows how to disable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to enable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to enable SGT tagging exemption for the L2 control protocols.

```
switch# configure terminal
switch(config)# interface ethernet 2/27
switch(config-if)# cts manual
switch(config-if-cts-manual)# no propagate-sgt l2-control
```

This example displays the error message when you enable SGT tagging exemption for the L2 protocols on non-supported modules:

```
switch# configure terminal
switch(config)# interface ethernet 7/2
switch(config-if)# cts manual
switch(config-if-cts-manual)# no propagate-sgt l2-control
ERROR: 'no propagate-sgt l2-control' is not allowed on any port of this line card type.
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec 802.1X configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

R Commands

radius abort

To discard a RADIUS Cisco Fabric Services distribution session in progress, use the **radius abort** command**.**

radius abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None

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 discard a RADIUS Cisco Fabric Services distribution session in progress:

```
switch# configure terminal
switch(config)# radius abort
```

Related Commands

Command	Description
show radius	Displays the RADIUS Cisco Fabric Services distribution status and other details.

radius commit

To apply the pending configuration pertaining to the RADIUS Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **radius commit** command**.**

radius commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Before committing the RADIUS configuration to the fabric, all switches in the fabric must have distribution enabled using the **radius distribute** command.

CFS does not distribute the RADIUS server group configurations, periodic RADIUS server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to initiate distribution of a RADIUS configuration to the switches in the fabric:

```
switch# configure terminal
switch(config)# radius commit
```

Related Commands

Command	Description
radius distribute	Enables Cisco Fabric Services distribution for RADIUS.
show radius	Displays the RADIUS Cisco Fabric Services distribution status and other details.

radius distribute

To enable Cisco Fabric Services distribution for RADIUS, use the **radius distribute** command. To disable this feature, use the **no** form of the command.

radius distribute

no radius distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

CFS does not distribute the RADIUS server group configurations, periodic RADIUS server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to enable RADIUS fabric distribution:

```
switch# configure terminal
switch(config)# radius distribute
```

This example shows how to disable RADIUS fabric distribution:

```
switch# configure terminal
switch(config)# no radius distribute
```

Related Commands

Command	Description
show radius distribution status	Displays the RADIUS Cisco Fabric Services distribution status.

radius-server deadtime

To configure the dead-time interval for all RADIUS servers on a Cisco NX-OS device, use the **radius-server deadtime** command. To revert to the default, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.

Command Default

0 minutes

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The dead-time interval is the number of minutes before the Cisco NX-OS device checks a RADIUS server that was previously unresponsive.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

The command does not require a license.

Examples

This example shows how to configure the global dead-time interval for all RADIUS servers to perform periodic monitoring:

```
switch# configure terminal
switch(config)# radius-server deadtime 5
```

This example shows how to revert to the default for the global dead-time interval for all RADIUS servers and disable periodic server monitoring:

```
switch# configure terminal
switch(config)# no radius-server deadtime 5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server directed-request

To allow users to send authentication requests to a specific RADIUS server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

radius-server directed-request

no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Sends the authentication request to the configured RADIUS server group

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can specify the *username @vrfname* :*hostname* during login, where vrfname is the virtual routing and forwarding (VRF) instance to use and hostname is the name of a configured RADIUS server. The username is sent to the RADIUS server for authentication.

This command does not require a license.

Examples

This example shows how to allow users to send authentication requests to a specific RADIUS serve when logging in:

```
switch# configure terminal
switch(config)# radius-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific RADIUS server when logging in:

```
switch# configure terminal
switch(config)# no radius-server directed-request
```

Related Commands

Command	Description
show radius-server directed-request	Displays the directed request RADIUS server configuration.

radius-server host

To configure RADIUS server parameters, use the **radius-server host** command. To revert to the default, use the **no** form of this command.

radius-server host {*hostname*| *ipv4-address*| *ipv6-address*} [**key** [**0**| **7**] *shared-secret* **[pac]**] **[accounting]** [**acct-port** *port-number*] [**auth-port** *port-number*] **[authentication]** [**retransmit** *count*] [**test** {**idle-time** *time*| **password** *password*| **username** *name*}] [**timeout** *seconds* [**retransmit** *count*]]

noradius-server host {*hostname*| *ipv4-address*| *ipv6-address*} [**key** [**0**| **7**] *shared-secret* **[pac]**] **[accounting]** [**acct-port** *port-number*] [**auth-port** *port-number*] **[authentication]** [**retransmit** *count*] [**test** {**idle-time** *time*| **password** *password*| **username** *name*}] [**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

hostname	RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	RADIUS server IPv4 address in the *A.B.C.D* format.
ipv6-address	RADIUS server IPv6 address in the *X:X:X::X* format.
key	(Optional) Configures the RADIUS server preshared secret key.
0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.
pac	(Optional) Enables the generation of Protected Access Credentials (PAC) on the RADIUS Cisco Access Control Server (ACS) for use with Cisco TrustSec.
accounting	(Optional) Configures accounting.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.

auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit *count*	(Optional) Configures the number of times that the device tries to connect to a RADIUS server(s) before reverting to local authentication. The range is from 1 to 5 times and the default is 1 time.
test	(Optional) Configures parameters to send test packets to the RADIUS server.
idle-time*time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password*password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username*name*	Specifies a username in the test packets. The name is alphanumeric, not case sensitive, and has a maximum of 32 characters.
timeout *seconds*	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 5 seconds and the range is from 1 to 60 seconds.

Command Default

Accounting port: 1813

Authentication port: 1812

Accounting: enabled

Authentication: enabled

Retransmission count: 1

Idle-time: none

Server monitoring: disabled

Timeout: 5 seconds

Test username: test

Test password: test

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

This command does not require a license.

Examples

This example shows how to configure RADIUS server authentication and accounting parameters:

```
switch# configure terminal
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003
switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure a RADIUS shared secret key, use the **radius-server key** command. To remove a configured shared secret, use the **no** form of this command.

radius-server key [**0**| **6**| **7**] *shared-secret*

no radius-server key [**0**| **6**| **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server.
6	(Optional) Configures a preshared key specified in type6 encrypted text to authenticate communication between the RADIUS client and server.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key used to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.

Command Default

Clear text

Command Modes

Global configuration

Command History

Release	Modification
5.2(1)	Added the
4.0(1)	This command was introduced.

Usage Guidelines

You must configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **radius-server host** command.

This command does not require a license.

Examples

This example shows how to provide various scenarios to configure RADIUS authentication:

```
switch# configure terminal
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server retransmit

To specify the number of times that the device should try a request with a RADIUS server, use the **radius-server retransmit** command. To revert to the default, use the **no** form of this command.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Number of times that the device tries to connect to a RADIUS server(s) before reverting to local authentication. The range is from 1 to 5 times.

Command Default

1 retransmission

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 configure the number of retransmissions to RADIUS servers:

```
switch# configure terminal
switch(config)# radius-server retransmit 3
```

This example shows how to revert to the default number of retransmissions to RADIUS servers:

```
switch# configure terminal
switch(config)# no radius-server retransmit 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server test

To monitor the availability of all RADIUS servers without having to configure the test parameters for each server individually, use the **radius-server test** command. To disable this configuration, use the **no** form of this command.

radius-server test {**idle-time** *time*| **password** *password*| **username** *name*}

no radius-server test {**idle-time** *time*| **password** *password*| **username** *name*}

Syntax Description

test	Configures parameters to send test packets to the RADIUS server.
idle-time*time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes. **Note** When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.
password*password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username*name*	Specifies a username in the test packets. The name is alphanumeric, not case sensitive, and has a maximum of 32 characters. **Note** To protect network security, we recommend that you use a username that is not the same as an existing username in the RADIUS database.

Command Default

Server monitoring: DisabledIdle time: 0 minutesTest username: test Test password: test

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable RADIUS authentication.

Any servers for which test parameters are not configured are monitored using the global level parameters.

Test parameters that are configured for individual servers take precedence over global test parameters.

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

This command does not require a license.

Examples

This example shows how to configure the parameters for global RADIUS server monitoring:

```
switch# configure terminal
switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server timeout

To specify the time between retransmissions to the RADIUS servers, use the **radius-server timeout** command. To revert to the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.

Command Default

1 second

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 configure the timeout interval:

```
switch# configure terminal
switch(config)# radius-server timeout 30
```

This example shows how to revert to the default interval:

```
switch# configure terminal
switch(config)# no radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

range

To specify a range of ports as a group member in an IP port object group, use the **range** command. To remove a port range group member from port object group, use the **no** form of this command.

[*sequence-number*] **range** *starting-port-number ending-port-number*

no {*sequence-number*| **range** *starting-port-number ending-port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
starting-port-number	Lowest port number that this group member matches. Valid values are from 0 to 65535.
ending-port-number	Highest port number that this group member matches. Valid values are from 0 to 65535.

Command Default

None

Command Modes

IP port object group configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether a **range** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 137 through port 139:

```
switch# configure terminal
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# range 137 139
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.
object-group ip port	Configures an IP port object group.
show object-group	Displays object groups.

rate-limit cpu direction

To configure rate limits globally on the device for packets that reach the supervisor module, use the **rate-limit cpu direction** command. To remove the rate limit configuration, use the **no** form of this command.

rate-limit cpu direction {**input**| **output**| **both**} **pps** *packets* **action log**

no rate-limit cpu direction {**input**| **output**| **both**} **pps** *packets* **action log**

Syntax Description

input	Specifies the maximum incoming packet rate.
output	Specifies the maximum outgoing packet rate.
both	Specifies the maximum incoming and outgoing packet rate.
pps	Specifies packets per second.
packets	Packets that reach the supervisor module. The range is from 1 to 100000.
action	Specifies the action to be taken when the rate of incoming or outgoing packets exceeds the configured rate limit.
log	Logs a system message when the rate of incoming or outgoing packets exceeds the configured rate limit.

Command Default

10000 packets per second

Command Modes

Global configuration

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

If the rate of incoming or outgoing packets exceeds the configured rate limit, the device logs a system message but does not drop any packets.

F1 Series modules support up to five rate limiters shared among all control traffic sent to the Supervisor module.

This command does not require a license.

Examples

This example shows how to configure rate limits globally on the device for packets that reach the supervisor module:

```
switch# configure terminal
switch(config)# rate-limit cpu direction both pps 10000 action log
switch(config)#
```

This example shows how to remove the global rate limit configuration:

```
switch# configure terminal
switch(config)# no rate-limit cpu direction both pps 10000 action log
switch(config)#
```

Related Commands

Command	Description
show system internal pktmgr internal control sw-rate-limit	Displays the inband and outband global rate limit configuration for packets that reach the supervisor module.

remark

To enter a comment into an IPv4, IPv6, or MAC access control list (ACL), use the **remark** command. To remove a **remark** command, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no {*sequence-number*| **remark** *remark*}

Syntax Description

sequence-number	(Optional) Sequence number of the **remark** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to remarks and rules.
remark	Text of the remark. This argument can be up to 100 alphanumeric, case-sensitive characters.

Command Default

No ACL contains a remark by default.

Command Modes

IP access-list configuration

IPv6 access-list configuration

MAC access-list configuration

Command History

Release	Modification
4.1(2)	Support for the IPv6 access-list configuration mode was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

The *remark* argument can be up to 100 characters. If you enter more than 100 characters for the *remark* argument, the device accepts the first 100 characters and drops any additional characters.

Examples

This example shows how to create a remark in an IPv4 ACL and display the results:

```
switch# configure terminal
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01

IP access list acl-ipv4-01
100 remark this ACL denies the marketing department access to the lab
ciscobox(config-acl)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
ipv6 access-list	Configures an IPv6 ACL
mac access-list	Configures a MAC ACL.
show access-list	Displays all ACLs or one ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.

replay-protection

To enable the data-path replay protection feature for Cisco TrustSec authentication on an interface, use the **replay-protection** command. To disable the data-path replay protection feature, use the **no** form of this command.

replay-protection

no replay-protection

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Cisco TrustSec 802.1X configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command is not supported for F1 Series modules and F2 Series modules.

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to enable data-path protect for Cisco TrustSec authentication on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to disable data-path protect for Cisco TrustSec authentication on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec 802.1X configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

resequence

To reassign sequence numbers to all rules in an access control list (ACL) or a time range, use the **resequence** command.

resequence *access-list-type* **access-list** *access-list-name starting-sequence-number increment*

resequence time-range *time-range-name starting-sequence-number increment*

Syntax Description

access-list-type	Type of the ACL. Valid values for this argument are the following keywords: • **arp** • **ip** • **ipv6** • **mac**
access-list *access-list-name*	Specifies the name of the ACL, which can be up to 64 alphanumeric, case-sensitive characters.
time-range*time-range-name*	Specifies the name of the time range, which can be up to 64 alphanumeric, case-sensitive characters.
starting-sequence-number	Sequence number for the first rule in the ACL or time range.
increment	Number that the device adds to each subsequent sequence number.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	Support for IPv6 ACLs was added.
4.0(1)	This command was introduced.

Usage Guidelines

The **resequence** command allows you to reassign sequence numbers to the rules of an ACL or time range. The new sequence number for the first rule is determined by the *starting-sequence-number* argument. Each additional rule receives a new sequence number determined by the *increment* argument. If the highest sequence number would exceed the maximum possible sequence number, then no sequencing occurs and the following message appears:

```
ERROR: Exceeded maximum sequence number.
```

The maximum sequence number is 4294967295.

This command does not require a license.

Examples

This example shows how to resequence an IPv4 ACL named ip-acl-01 with a starting sequence number of 100 and an increment of 10, using the **show ip access-lists** command to verify sequence numbering before and after the use of the **resequence** command:

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

IP access list ip-acl-01
        7 permit tcp addrgroup lab-machines any
        10 permit udp addrgroup lab-machines any
        13 permit icmp addrgroup lab-machines any
        17 deny igmp any any

switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp addrgroup lab-machines any
        110 permit udp addrgroup lab-machines any
        120 permit icmp addrgroup lab-machines any
        130 deny igmp any any
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip access-list	Configures an IPv4 ACL.
ipv6 access-list	Configures an IPv6 ACL.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

revocation-check

To configure trustpoint revocation check methods, use the **revocation-check** command. To discard the revocation check configuration, use the **no** form of this command.

revocation-check {**crl [none]|| none**}

no revocation-check {**crl [none]|| none**}

Syntax Description

crl	Specifies the locally stored certificate revocation list (CRL) as the place to check for revoked certificates.
none	(Optional) Specifies that no checking is performed for revoked certificates.

Command Default

By default, the revocation checking method for a trustpoint is CRL.

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

A revocation check can perform one or more of the methods which you specify as an ordered list. During peer certificate verification, each method is tried in the specified order until one method succeeds by providing the revocation status. When you specify **none** as the method, it means that there is no need to check the revocation status, and the peer certificate is not revoked. If **none** is the first method that you specify in the method list, you cannot specify subsequent methods because checking is not required.

This command does not require a license.

Examples

This example shows how to check for revoked certificates in the locally stored CRL:

```
switch(config-trustpoint)# revocation-check crl
```

This example shows how to do no checking for revoked certificates:

```
switch(config-trustpoint)# revocation-check none
```

Related Commands

Command	Description
crypto ca crl-request	Configures a CRL or overwrites the existing one for the trustpoint CA.

Command	Description
show crypto ca crl	Displays configured CRLs.

role abort

To discard a user role Cisco Fabric Services distribution session in progress, use the **role abort** command.

role abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None

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 discard a user role Cisco Fabric Services distribution session in progress:

```
switch# configure terminal
switch(config)# role abort
```

Related Commands

Command	Description
show role	Displays the user role Cisco Fabric Services distribution status and other details.

role commit

To apply the pending configuration pertaining to the user role Cisco Fabric Services distribution session in progress in the fabric, use the **role commit** command**.**

role commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Before committing the user role configuration to the fabric, all switches in the fabric must have distribution enabled using the **role distribute** command.

This command does not require a license.

Examples

This example shows how to initiate distribution of a user role configuration to the switches in the fabric:

```
switch# configure terminal
switch(config)# role commit
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for user roles.
show role	Displays the user role Cisco Fabric Services distribution status and other details.

role distribute

To enable Cisco Fabric Services distribution for user roles, use the **role distribute** command. To disable this feature, use the **no** form of the command.

role distribute

no role distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled

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 enable role fabric distribution:

```
switch# configure terminal
switch(config)# role distribute
```

This example shows how to disable role fabric distribution:

```
switch# configure terminal
switch(config)# no role distribute
```

Related Commands

Command	Description
show role distribution status	Displays role Cisco Fabric Services distribution status.

role feature-group name

To create or specify a user role feature group and enter user role feature group configuration mode, use the **role feature-group name** command. To delete a user role feature group, use the **no** form of this command.

role feature-group name *group-name*

no role feature-group name *group-name*

Syntax Description

group-name	User role feature group name. The *group-name* has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software provides the default user role feature group L3 for Layer 3 features. You cannot modify or delete the L3 user role feature group.

This command does not require a license.

Examples

This example shows how to create a user role feature group and enter user role feature group configuration mode:

```
switch# configure terminal
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

This example shows how to remove a user role feature group:

```
switch# configure terminal
switch(config)# no role feature-group name MyGroup
```

Related Commands

Command	Description
feature-group name	Specifies or creates a user role feature group and enters user role feature group configuration mode.

Command	Description
show role feature-group	Displays the user role feature groups.

role name

To create or modify a user role or privilege role and enter user role configuration mode, use the **role name** command. To delete a user role, use the **no** form of this command.

role name {*role-name*| **priv-n**}

no role name {*role-name*| **priv-n**}

Syntax Description

role-name	User role name. The *role-name* argument has a maximum length of 16 characters and is a case-sensitive, alphanumeric character string.
priv-*n*	Specifies the privilege level. The *n* argument is a number between 0 and 13.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	The **priv-***n* keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software provides four default user roles:

- network-admin—Complete read-and-write access to the entire Cisco NX-OS device (only available in the default VDC)
- network-operator—Complete read access to the entire Cisco NX-OS device (only available in the default VDC)
- vdc-admin—Read-and-write access limited to a VDC
- vdc-operator—Read access limited to a VDC

You cannot change or remove the default user roles.

You must follow these guidelines when changing the rules of privilege roles:

- You cannot modify the priv-14 and priv-15 roles.
- You can add deny rules only to the priv-0 role.

- These commands are always permitted for the priv-0 role: **configure**, **copy**, **dir**, **enable**, **ping**, **show**, **ssh**, **telnet**, **terminal**, **traceroute**, **end**, and **exit**.

This command does not require a license.

Examples

This example shows how to create a user role and enter user role configuration mode:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)#
```

This example shows how to remove a user role:

```
switch# configure terminal
switch(config)# no role name MyRole
```

This example shows how to enable privilege level 5 for users:

```
switch# configure terminal
switch(config)# role name priv-5
switch(config-role)#
```

Related Commands

Command	Description
rule	Configure rules for a user role or for users of privilege roles.
show role	Displays the user roles.

router-preference maximum

To verify the advertised default router preference parameter value, use the **router-preference maximum** command in RA guard policy configuration mode.

router-preference maximum {**high**| **low**| **medium**}

Syntax Description

high	Default router preference parameter value is higher than the specified limit.
medium	Default router preference parameter value is equal to the specified limit.
low	Default router preference parameter value is lower than the specified limit.

Command Default

The router preference maximum value is not configured.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **router-preference maximum** command enables verification that the advertised default router preference parameter value is lower than or equal to a specified limit. You can use this command to give a lower priority to default routers advertised on trunk ports, and to give precedence to default routers advertised on access ports.

The **router-preference maximum** command limit are high, medium, or low. If, for example, this value is set to **medium** and the advertised default router preference is set to **high** in the received packet, then the packet is dropped. If the command option is set to **medium** or **low** in the received packet, then the packet is not dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures router-preference maximum verification to be high:

```
switch(config)# ipv6 nd raguard policy raguard1
switch(config-ra-guard)# router-preference maximum high
```

Related Commands

Command	Description
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

rsakeypair

To configure and associate the RSA key pair details to a trustpoint, use the **rsakeypair** command. To disassociate the RSA key pair from the trustpoint, use the **no** form of this command.

rsakeypair *key-pair-label [key-pair-size]*

no rsakeypair *key-pair-label [key-pair-size]*

Syntax Description

key-pair-label	Name for the RSA key pair. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
key-pair-size	(Optional) Size for the RSA key pair. The size values are 512, 768, 1024, 1536, and 2048 bits.

Command Default

The default key pair size is 512 if the key pair is not already generated.

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You can associate only one RSA key pair with a trustpoint CA, even though you can associate the same key pair with many trustpoint CAs. This association must occur before you enroll with the CA to obtain an identity certificate. If the key pair was previously generated (using the **crypto key generate** command), then the key pair size, if specified, should be the same size as that was used during the generation. If the specified key pair is not yet generated, you can enter the **crypto ca enroll** command to generated the RSA key pair during the enrollment.

Note The **no** form of the **rsakeypair** command disassociates the key pair from the trustpoint. Before you enter the **no rsakeypair** command, first remove the identity certificate, if present, from the trustpoint CA to ensure that the association between the identity certificate and the key pair for a trustpoint is consistent.

This command does not require a license.

Examples

This example shows how to associate an RSA key pair to a trustpoint:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# rsakeypair adminid-key
```

This example shows how to disassociate an RSA key pair from a trustpoint:

```
switch(config-trustpoint)# no rsakeypair adminid-key
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch's RSA key pair created for the trustpoint CA.
crypto key generate rsa	Configures RSA key pair information.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

rule

To configure rules for a user role or for users of privilege roles, use the **rule** command. To delete a rule, use the **no** form of this command.

rule *number* {**deny**| **permit**} {**command** *command-string*| {**read**| **read-write**} **oid** *snmp_oid_name* [**feature** *feature-name*| **feature-group** *group-name*]}

no rule *number*

Syntax Description

number	Sequence number for the rule. The Cisco NX-OS software applies the rule with the highest value first and then the rest in descending order. The range is 1 to 256.
deny	Denies access to commands or features.
permit	Permits access to commands or features.
command *command-string*	Specifies a command string.
read	Specifies read access.
read-write	Specifies read and write access.
oid *snmp_oid_name*	Specifies a read-only or read-and-write-rule for an SNMP object identifier (OID). The range it 1 to 32 elements.
feature *feature-name*	(Optional) Specifies a feature name. Use the **show role feature** command to list the Cisco NX-OS feature names.
feature-group *group-name*	(Optional) Specifies a feature group.

Command Default

None

Command Modes

User role configuration

Command History

Release	Modification
4.0(1)	This command was introduced.
6.0(1)	Added the **oid** keyword.

Usage Guidelines

You can configure up to 256 rules for each role.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

This command does not require a license.

Examples

This example shows how to add rules to a user role:

```
switch# configure terminal
switch(config)# role MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

This example shows how to remove rule from a user role:

```
switch# configure terminal
switch(config)# role MyRole
switch(config-role)# no rule 10
```

Related Commands

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

S Commands

sak-expiry-time

To set an expiry time for a forced Secure Association Key (SAK) rekey, use the **sak-expiry-time** command. To reset to the default expiry time, use the **no** form of this command.

sak-expiry-time *time*

no sak-expiry-time *time*

Syntax Description

time	Time, in seconds, to force a SAK rekey. The range is 1-2592000. The default is pn-exhaust.

Command Default

The default value is pn-exhaust.

Command Modes

MACsec policy configuration (config-macsec-policy)

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To use this command, you should enable the MKA feature first.

Examples

This example shows how to set the SAK expiry time:

```
switch# configure terminal
switch(config)# macsec policy p1
switch(config-macsec-policy)# sak-expiry-time 60
```

Related Commands

Command	Description
cipher suite	Configures the cipher suite for encrypting traffic with MACsec.
conf-offset	Configures the confidentiality offset for MKA encryption.
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.

Command	Description
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
key-octet-string	Configures the text for a MACsec key.
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

sap modelist

To configure the Cisco TrustSec Security Association Protocol (SAP) operation mode, use the **sap modelist** command. To revert to the default, use the **no** form of this command.

sap modelist {**gcm-encrypt**| **gmac**| **no-encap**| **none**}

no sap modelist {**gcm-encrypt**| **gmac**| **no-encap**| **none**}

Syntax Description

gcm-encrypt	Specifies Galois/Counter Mode (GCM) encryption and authentication mode.
gmac	Specifies GCM authentication mode.
no-encap	Specifies no encapsulation and no security group tag (SGT) insertion.
none	Specifies the encapsulation of the SGT without authentication or encryption.

Command Default

gcm-encrypt

Command Modes

Cisco TrustSec 802.1X configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to configure Cisco TrustSec SAP operation mode on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# sap modelist gmac
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to revert to the default Cisco TrustSec SAP operation mode on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no sap modelist gmac
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec 802.1X configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

sap pmk

To manually configure the Cisco TrustSec Security Association Protocol (SAP) pairwise master key (PMK), use the **sap pmk** command. To remove the SAP configuration, use the **no** form of this command.

sap pmk [*key*| **[left-zero-padded]** [**display encrypt**]| **encrypted** {**encrypted_pmk| use-dot1x**} [**modelist** {**gcm-encrypt| gmac| no-encap| null**}]]

no sap

Syntax Description

key	Key value. This is a hexadecimal string with an even number of characters. The maximum length is 32 characters.
left-zero-padded	(Optional) Pads zeros to the left of the entered string if the PMK length is less than 32 bytes.
display encrypt	(Optional) Specifies that the configured PMK be displayed in AES-encrypted format in the running configuration.
encrypted encrypted_pmk	Specifies an encrypted PMK string of 64 bytes (128 hexadecimal characters).
use-dot1x	Specifies that the peer device does not support Cisco TrustSec 802.1X authentication or authorization but does support SAP data path encryption and authentication.
modelist	(Optional) Specifies the SAP operation mode.
gcm-encrypt	Specifies Galois/Counter Mode (GCM) encryption and authentication mode.
gmac	Specifies GCM authentication mode.
no-encap	Specifies no encapsulation and no security group tag (SGT) insertion.
null	Specifies the encapsulation of the SGT without authentication or encryption.

Command Default

gcm-encrypt

Command Modes

Cisco TrustSec manual configuration

Command History

Release	Modification
6.2(2)	The left-zero-padded, display encrypt and encrypted encrypted_pmk keywords and argument were added.
4.0(3)	The **use-dot1x** keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command is not supported for F1 Series modules and F2 Series modules.

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to manually configure Cisco TrustSec SAP on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to remove a manual Cisco TrustSec SAP configuration from an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no sap
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
cts manual	Enters Cisco TrustSec manual configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

send-lifetime

To specify the time interval within which the device sends the key during key exchange with another device, use the **send-lifetime** command. To remove the time interval, use the **no** form of this command.

send-lifetime [local] *start-time* [**duration** *duration-value*| **infinite**| *end-time*]

Syntax Description

local	(Optional) Specifies that the device treats the configured times as local times. By default, the device treats the *start-time* and *end-time* arguments as UTC.
start-time	Time of day and date that the key becomes active. For information about the values for the *start-time* argument, see the "Usage Guidelines" section.
duration *duration-value*	(Optional) Specifies the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).
infinite	(Optional) Specifies that the key never expires.
end-time	(Optional) Time of day and date that the key becomes inactive. For information about valid values for the *end-time* argument, see the "Usage Guidelines" section.

Command Default

infinite

Command Modes

Key configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

By default, the device interprets all time range rules as UTC.

By default, the time interval within which the device sends a key during key exchange with another device—the send lifetime—is infinite, which means that the key is always valid.

The *start-time* and *end-time* arguments both require time and date components, in the following format:

hour[:*minute*[:*second*]] *month day year*

You specify the hour in 24-hour notation. For example, in 24-hour notation, 8:00 a.m. is 8:00 and 8:00 p.m. is 20:00. The minimum valid *start-time* is 00:00:00 Jan 1 1970, and the maximum valid *start-time* is 23:59:59 Dec 31 2037.

Examples

This example shows how to create a send lifetime that begins at midnight on June 13, 2008, and ends at 11:59:59 p.m. on August 12, 2008:

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# send-lifetime 00:00:00 Jun 13 2008 23:59:59 Aug 12 2008
switch(config-keychain-key)#
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
key	Configures a key.
key chain	Configures a keychain.
key-string	Configures a key string.
show key chain	Displays keychain configuration.

server

To add a server to a RADIUS, TACACS+, or Lightweight Directory Access Protocol (LDAP) server group, use the **server** command. To delete a server from a server group, use the **no** form of this command.

server {*ipv4-address*| *ipv6-address*| *hostname*}

no server {*ipv4-address*| *ipv6-address*| *hostname*}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X::X* format.
hostname	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

RADIUS server group configurationTACACS+ server group configurationLDAP server group configuration

Command History

Release	Modification
5.0(2)	Support for LDAP server groups was added.
4.0(1)	This command was introduced.

Usage Guidelines

You can configure up to 64 servers in a server group.

Use the **aaa group server radius** command to enter RADIUS server group configuration mode, the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode, or the **aaa group server ldap** command to enter LDAP server group configuration mode.

If the server is not found, use the **radius-server host** command, **tacacs-server host** command, or **ldap-server host** command to configure the server.

Note You must use the **feature tacacs+** command before you configure TACACS+ and the **feature ldap** command before you configure LDAP.

This command does not require a license.

Examples

This example shows how to add a server to a RADIUS server group:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
```

This example shows how to delete a server from a RADIUS server group:

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 10.10.1.1
```

This example shows how to add a server to a TACACS+ server group:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
```

This example shows how to delete a server from a TACACS+ server group:

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 10.10.2.2
```

This example shows how to add a server to an LDAP server group:

```
switch# configure terminal
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-ldap)# server 10.10.3.3
```

This example shows how to delete a server from an LDAP server group:

```
switch# configure terminal
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-ldap)# no server 10.10.3.3
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures a RADIUS server.
show ldap-server groups	Displays LDAP server group information.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
feature tacacs+	Enables TACACS+.
tacacs-server host	Configures a TACACS+ server.
feature ldap	Enables LDAP.
ldap-server host	Configures an LDAP server.

service dhcp

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

service dhcp

no service dhcp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.2(1)	This command was deprecated and replaced with the **ip dhcp relay** command.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to globally enable DHCP snooping:

```
switch# configure terminal
switch(config)# service dhcp
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.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping	Displays general information about DHCP snooping.

Command	Description
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

service-policy input

To attach a control plane policy map to the control plane, use the **service-policy input** command. To remove a control plane policy map, use the **no** form of this command.

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

Syntax Description

policy-map-name	Name of the control plane policy map.

Command Default

None

Command Modes

Control plane configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

You can assign only one control place policy map to the control plane. To assign a new control plane policy map to the control plane, you must remove the old control plane policy map.

This command does not require a license.

Examples

This example shows how to assign a control plane policy map to the control plane:

```
switch# configure terminal
switch(config)# control-plane
switch(config-cp)# service-policy input PolicyMapA
```

This example shows how to remove a control plane policy map from the control plane:

```
switch# configure terminal
switch(config)# control-plane
switch(config-cp)# no service-policy input PolicyMapA
```

Related Commands

Command	Description
policy-map type control-plane	Specifies a control plane policy map and enters policy map configuration mode.

Command	Description
show policy-map type control-plane	Displays configuration information for control plane policy maps.

set cos

To set the IEEE 802.1Q class of service (CoS) value for a control plane policy map, use the **set cos** command. To revert to the default, use the **no** form of this command.

set cos [inner] *cos-value*

no set cos [inner] *cos-value*

Syntax Description

inner	(Optional) Specifies the inner 802.1Q in a Q-in-Q environment.
cos-value	Numerical value of CoS in the control plane policy map. The range is from 0 to 7.

Command Default

0

Command Modes

Policy map class configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to configure the CoS value for a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set cos 4
```

This example shows how to revert to the default CoS value for a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set cos 4
```

Related Commands

Command	Description
class (policy map)	Specifies a control plane class map for a control plane policy map and enters policy map class configuration mode.
policy-map type control-plane	Specifies a control plane policy map and enters policy map configuration mode.
show policy-map type control-plane	Displays configuration information for control plane policy maps.

set dscp (policy map class)

To set the differentiated services code point (DSCP) value for IPv4 and IPv6 packets in a control plane policy map, use the **set dscp** command. To revert to the default, use the **no** form of this command.

set dscp [tunnel] {*dscp-value*| **af11**| **af12**| **af13**| **af21**| **af22**| **af23**| **af31**| **af32**| **af33**| **af41**| **af42**| **af43**| **cs1**| **cs2**| **cs3**| **cs4**| **cs5**| **cs6**| **cs7**| **ef**| **default**}

no set dscp [tunnel] {*dscp-value*| **af11**| **af12**| **af13**| **af21**| **af22**| **af23**| **af31**| **af32**| **af33**| **af41**| **af42**| **af43**| **cs1**| **cs2**| **cs3**| **cs4**| **cs5**| **cs6**| **cs7**| **ef**| **default**}

Syntax Description

tunnel	(Optional) Sets DSCP in a tunnel encapsulation.
dscp-value	Numerical value of CoS in the control plane policy map. The range is from 0 to63.
af11	Specifies assured forwarding 11 DSCP (001010).
af12	Specifies assured forwarding 12 DSCP (001100).
af13	Specifies assured forwarding 13 DSCP (001110).
af21	Specifies assured forwarding 21 DSCP (010010).
af22	Specifies assured forwarding 22 DSCP (010100).
af23	Specifies assured forwarding 23 DSCP (010110).
af31	Specifies assured forwarding 31 DSCP (011010).
af32	Specifies assured forwarding 32 DSCP (011100).
af33	Specifies assured forwarding 33 DSCP (011110).
af41	Specifies assured forwarding 41 DSCP (100010).
af42	Specifies assured forwarding 42 DSCP (100100).
af43	Specifies assured forwarding 43 DSCP (100110).
cs1	Specifies class selector 1 (precedence 1) DSCP (001000).
cs2	Specifies class selector 2 (precedence 2) DSCP (010000).
cs3	Specifies class selector 3 (precedence 3) DSCP (011000).

cs4	Specifies class selector 4 (precedence 4) DSCP (100000).
cs5	Specifies class selector 5 (precedence 5) DSCP (101000).
cs6	Specifies class selector 6 (precedence 6) DSCP (110000).
cs7	Specifies class selector 7 (precedence 7) DSCP (111000).
ef	Specifies expedited forwarding DSCP (101110).
default	Specifies default DSCP (000000).

Command Default

default

Command Modes

Policy map class configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to configure the DSCP value for a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set dscp 4
```

This example shows how to revert to the default DSCP value for a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set dscp 4
```

Related Commands

Command	Description
class (policy map)	Specifies a control plane class map for a control plane policy map and enters policy map class configuration mode.
policy-map type control-plane	Specifies a control plane policy map and enters policy map configuration mode.
show policy-map type control-plane	Displays configuration information for control plane policy maps.

set precedence (policy map class)

To set the precedence value for IPv4 and IPv6 packets in a control plane policy map, use the **set precedence** command. To revert to the default, use the **no** form of this command.

set precedence [tunnel] {*prec-value*| **critical**| **flash**| **flash-override**| **immediate**| **internet**| **network**| **priority**| **routine**}

no set precedence [tunnel] {*prec-value*| **critical**| **flash**| **flash-override**| **immediate**| **internet**| **network**| **priority**| **routine**}

Syntax Description

tunnel	(Optional) Sets the precedence in a tunnel encapsulation.
prec-value	Numerical value for DSCP precedence in the control plane policy map. The range is from 0 to 7.
critical	Specifies critical precedence equal to precedence value 5.
flash	Specifies flash precedence equal to precedence value 3.
flash-override	Specifies flash override precedence equal to precedence value 4.
immediate	Specifies immediate precedence equal to precedence value 2.
internet	Specifies internet precedence equal to precedence value 6.
network	Specifies network precedence equal to precedence value 7.
priority	Specifies priority precedence equal to precedence value 1.
routine	Specifies routine precedence equal to precedence value 0.

Command Default

0 or routine

Command Modes

Policy map class configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to configure the CoS value for a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set precedence critical
```

This example shows how to revert to the default CoS value for a control plane policy map:

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set precedence critical
```

Related Commands

Command	Description
class (policy map)	Specifies a control plane class map for a control plane policy map and enters policy map class configuration mode.
policy-map type control-plane	Specifies a control plane policy map and enters policy map configuration mode.
show policy-map type control-plane	Displays configuration information for control plane policy maps.

source-interface

To assign a source interface for a specific RADIUS or TACACS+ server group, use the **source-interface** command. To revert to the default, use the **no** form of this command.

source-interface *interface*

no source-interface

Syntax Description

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

Command Default

The default is the global source interface.

Command Modes

RADIUS configurationTACACS+ configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

The **source-interface** command to override the global source interface assigned by the **ip radius source-interface** command or **ip tacacs source-interface** command.

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

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 radius source-interface mgmt 0
switch(config-radius)# source-interface ethernet 2/1
```

Related Commands

Command	Description
feature tacacs+	Enables the TACACS+ feature.
ip radius source-interface	Configures the global source interface for the RADIUS groups configured on the Cisco NX-OS device.

Command	Description
ip tacacs source-interface	Configures the global source interface for the TACACS+ groups configured on the Cisco NX-OS device.
show radius-server groups	Displays the RADIUS server group configuration.
show tacacs-server groups	Displays the TACACS+ server group configuration.

ssh

To create a Secure Shell (SSH) session on the Cisco NX-OS device, use the **ssh** command.

ssh [*username* @] {*ipv4-address*| *hostname*} [**vrf** *vrf-name*]

Syntax Description

username	(Optional) Username for the SSH session. The username is not case sensitive.
ipv4-address	IPv4 address of the remote device.
hostname	Hostname of the remote device. The hostname is case sensitive.
vrf*vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH session. The VRF name is case sensitive.

Command Default

Default VRF

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

To use IPv6 addressing for an SSH session, use the **ssh6** command.

The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

If you are planning to create an SSH session to a remote device from the boot mode of a Cisco NX-OS device, you must obtain the hostname for the remote device, enable the SSH server on the remote device, and ensure that the Cisco NX-OS device is loaded with only the kickstart image.

This command does not require a license.

Examples

This example shows how to start an SSH session using IPv4:

```
switch# ssh 10.10.1.1 vrf management
```

```
The authenticity of host '10.10.1.1 (10.10.1.1)' can't be established.
RSA key fingerprint is 9b:d9:09:97:f6:40:76:89:05:15:42:6b:12:48:0f:d6.
```

```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.1.1' (RSA) to the list of known hosts.
User Access Verification
Password:
```

This example shows how to create an SSH session to a remote device from the boot mode of the Cisco NX-OS device:

```
switch(boot)# ssh user1@10.10.1.1
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
copy scp:	Copies a file from the Cisco NX-OS device to a remote device using the Secure Copy Protocol (SCP).
feature ssh	Enables the SSH server.
ssh6	Starts an SSH session using IPv6 addressing.

ssh key

To create a Secure Shell (SSH) server key for a virtual device context (VDC), use the **ssh key** command. To remove the SSH server key, use the **no** form of this command.

ssh key {**dsa [force]**| **rsa** [*length* **[force]**]}

no ssh key [**dsa**| **rsa**]

Syntax Description

dsa	Specifies the Digital System Algrorithm (DSA) SSH server key.
force	(Optional) Forces the replacement of an SSH key.
rsa	Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key.
length	(Optional) Number of bits to use when creating the SSH server key. The range is from 1024 to 2048.

Command Default

1024-bit length

Command Modes

Global configuration

Command History

Release	Modification
5.1(1)	Removed support for RSA keys less than 1024 bits.
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

If you want to remove or replace an SSH server key, you must first disable the SSH server using the **no feature ssh** command.

This command does not require a license.

Examples

This example shows how to create an SSH server key using DSA:

```
switch# configure terminal
switch(config)# ssh key dsa
generating dsa key(1024 bits).....
..
generated dsa key
```

This example shows how to create an SSH server key using RSA with the default key length:

```
switch# configure terminal
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
switch# configure terminal
switch(config)# ssh key rsa 1024
generating rsa key(1024 bits).....
.
generated rsa key
```

This example shows how to replace an SSH server key using DSA with the force option:

```
switch# configure terminal
switch(config)# no feature ssh
switch(config)# ssh key dsa force
deleting old dsa key.....
generating dsa key(1024 bits).....
.
generated dsa key
switch(config)# feature ssh
```

This example shows how to remove the DSA SSH server key:

```
switch# configure terminal
switch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
switch(config)# no ssh key dsa
switch(config)# feature ssh
```

This example shows how to remove all SSH server keys:

```
switch# configure terminal
switch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
switch(config)# no ssh key
switch(config)# feature ssh
```

Related Commands

Command	Description
show ssh key	Displays the SSH server key information.
feature ssh	Enables the SSH server.

ssh login-attempts

To configure the maximum number of times that a user can attempt to log in to a Secure Shell (SSH) session, use the **ssh login-attempts** command. To disable the configuration, use the **no** form of this command.

ssh login-attempts *number*

no ssh login-attempts

Syntax Description

number	Maximum number of login attempts. The range is from 1 to 10.

Command Default

3

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

The total number of login attempts includes attempts through public-key authentication, certificate-based authentication, and password-based authentication.

This command does not require a license.

If the user exceeds the maximum number of permitted login attempts, the session disconnects.

Examples

This example shows how to configure the maximum number of times that a user can attempt to log in to an SSH session:

```
switch# configure terminal
switch(config)# ssh login-attempts 5
```

This example shows how to disable the SSH login attempt configuration:

```
switch# configure terminal
switch(config)# no ssh login-attempts
```

Related Commands

Command	Description
show running-config security all	Displays the configured maximum number of SSH login attempts.

ssh server enable

To enable the Secure Shell (SSH) server for a virtual device context (VDC), use the **ssh server enable** command. To disable the SSH server, use the **no** form of this command.

ssh server enable

no ssh server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was deprecated and replaced with the **feature ssh** command.
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

This command does not require a license.

Examples

This example shows how to enable the SSH server:

```
switch# configure terminal
switch(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
switch# configure terminal
switch(config)# no ssh server enable

XML interface to system may become unavailable since ssh is disabled
```

Related Commands

Command	Description
show ssh server	Displays the SSH server key information.

ssh6

To create a Secure Shell (SSH) session using IPv6 on the Cisco NX-OS device, use the **ssh6** command.

ssh6 [*username @*] {*ipv6-address*| *hostname*} [**vrf** *vrf-name*]

Syntax Description

username	(Optional) Username for the SSH session. The username is not case sensitive.
ipv6-address	IPv6 address of the remote device.
hostname	Hostname of the remote device.
vrf*vrf-name*	(Optional) Specifies the virtual forwarding and routing (VRF) name to use for the SSH session. The VRF name is case sensitive.

Command Default

Default VRF

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

To use IPv4 addressing to start an SSH session, use the **ssh** command.

The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

This command does not require a license.

Examples

This example shows how to start an SSH session using IPv6:

```
switch# ssh host2 vrf management
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.

Command	Description
ssh	Starts an SSH session using IPv4 addressing.
feature ssh	Enables the SSH server.

statistics per-entry

To start recording statistics for how many packets are permitted or denied by each entry in an IP, a MAC access control list (ACL), or a VLAN access-map entry, use the **statistics per-entry** command. To stop recording per-entry statistics, use the **no** form of this command.

statistics per-entry

no statistics per-entry

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

IP access-list configuration

IPv6 access-list configuration

MAC access-list configuration

VLAN access-map configuration

Command History

Release	Modification
4.0(3)	Changed command from **statistics** to **statistics per-entry**.
4.0(1)	This command was introduced.

Usage Guidelines

When the device determines that an IPv4, IPv6, MAC, or VLAN ACL applies to a packet, it tests the packet against the conditions of all entries in the ACLs. ACL entries are derived from the rules that you configure with the applicable **permit** and **deny** commands. The first matching rule determines whether the packet is permitted or denied. Enter the **statistics per-entry** command to start recording how many packets are permitted or denied by each entry in an ACL.

Statistics are not supported if the DHCP snooping feature is enabled.

The device does not record statistics for implicit rules. To record statistics for these rules, you must explicitly configure an identical rule for each implicit rule. For more information about implicit rules, see the following commands:

- **ip access-list**
- **ipv6 access-list**
- **mac access-list**

To view per-entry statistics, use the **show access-lists** command or the applicable following command:

- **show ip access-lists**
- **show ipv6 access-lists**
- **show mac access-lists**

To clear per-entry statistics, use the **clear access-list counters** command or the applicable following command:

- **clear ip access-list counters**
- **clear ipv6 access-list counters**
- **clear mac access-list counters**
- **clear vlan access-list counters**

This command does not require a license.

Examples

This example shows how to start recording per-entry statistics for an IPv4 ACL named ip-acl-101:

```
switch(config)# ip access-list ip-acl-101
switch(config-acl)# statistics per-entry
switch(config-acl)#
```

This example shows how to stop recording per-entry statistics for an IPv4 ACL named ip-acl-101:

```
switch(config)# ip access-list ip-acl-101
switch(config-acl)# no statistics per-entry
switch(config-acl)#
```

This example shows how to start recording per-entry statistics for the ACLs in entry 20 in a VLAN access-map named vlan-map-01:

```
switch(config)# vlan access-map vlan-map-01 20
switch(config-access-map)# statistics per-entry
switch(config-access-map)#
```

This example shows how to stop recording per-entry statistics for the ACLs in entry 20 in a VLAN access-map named vlan-map-01:

```
switch(config)# vlan access-map vlan-map-01 20
switch(config-access-map)# no statistics per-entry
switch(config-access-map)#
```

Related Commands

Command	Description
show access-lists	Displays all IPv4, IPv6, and MAC ACLs, or a specific ACL.
clear access-list counters	Clears per-entry statistics for all IPv4, IPv6, and MAC ACLs, or for a specific ACL.

storm-control level

To set the suppression level for traffic storm control, use the **storm-control level** command. To turn off the suppression mode or revert to the default, use the **no** form of this command.

storm-control {**broadcast**| **multicast**| **unicast**} **level** *percentage* [. *fraction*]

no storm-control {**broadcast**| **multicast**| **unicast**} **level**

Syntax Description

broadcast	Specifies the broadcast traffic.
multicast	Specifies the multicast traffic.
unicast	Specifies the unicast traffic.
percentage	Percentage of the suppression level. The range is from 0 to 100 percent.
. *fraction*	(Optional) Fraction of the suppression level. The range is from 0 to 99.

Command Default

All packets are passed

Command Modes

Interface configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Enter the **storm-control level** command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

Only one suppression level is shared by all three suppression modes. For example, if you set the broadcast level to 30 and set the multicast level to 40, both levels are enabled and set to 40.

The period (.) is required when you enter the fractional-suppression level.

The suppression level is a percentage of the total bandwidth. A threshold value of 100 percent means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port.

Use the **show interfaces counters broadcast** command to display the discard count.

Use one of the follow methods to turn off suppression for the specified traffic type:

- Set the level to 100 percent for the specified traffic type.
- Use the **no** form of this command.

This command does not require a license.

Examples

This example shows how to enable suppression of broadcast traffic and set the suppression threshold level:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# storm-control broadcast level 30
```

This example shows how to disable the suppression mode for multicast traffic:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no storm-control multicast level
```

Related Commands

Command	Description
show interface	Displays the storm-control suppression counters for an interface.
show running-config	Displays the configuration of the interface.

switchport port-security

To enable port security on a Layer 2 Ethernet interface or Layer 2 port-channel interface, use the **switchport port-security** command. To remove port security configuration, use the **no** form of this command.

switchport port-security

no switchport port-security

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

Per interface, port security is disabled by default.

You must configure the interface as a Layer 2 interface by using the **switchport** command before you can use the **switchport port-security** command.

You must enable port security by using the **feature port-security** command before you can use the **switchport port-security** command.

If port security is enabled on any member port of the Layer 2 port-channel interface, the device does not allow you to disable port security on the port-channel interface. To do so, remove all secure member ports from the port-channel interface first. After disabling port security on a member port, you can add it to the port-channel interface again, as needed.

Enabling port security on an interface also enables the default method for learning secure MAC addresses, which is the dynamic method. To enable the sticky learning method, use the **switchport port-security mac-address sticky** command.

This command does not require a license.

Examples

This example shows how to enable port security on the Ethernet 2/1 interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security
switch(config-if)#
```

This example shows how to enable port security on the port-channel 10 interface:

```
switch# configure terminal
switch(config)# interface port-channel 10
switch(config-if)# switchport port-security
switch(config-if)#
```

Related Commands

Command	Description
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security aging time	Configures the aging time for dynamically learned, secure MAC addresses.
switchport port-security aging type	Configures the aging type for dynamically learned, secure MAC addresses.
switchport port-security mac-address	Configures a static MAC address.
switchport port-security mac-address sticky	Enables the sticky method for learning secure MAC addresses.
switchport port-security maximum	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
switchport port-security violation	Configures the security violation action for an interface.

switchport port-security aging type

To configure the aging type for dynamically learned, secure MAC addresses, use the **switchport port-security aging type** command. To return to the default aging type, which is absolute aging, use the **no** form of this command.

switchport port-security aging type {**absolute| inactivity**}

no switchport port-security aging type {**absolute| inactivity**}

Syntax Description

absolute	Specifies that the dynamically learned, secure MAC addresses age is based on how long ago the device learned the address.
inactivity	Specifies that the dynamically learned, secure MAC addresses age is based on how long ago the device last received traffic from the MAC address on the current interface.

Command Default

absolute

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

The default aging type is absolute aging.

You must enable port security by using the **feature port-security** command before you can use the **switchport port-security aging type** command.

Before using this command, you must use the **switchport** command to configure the interface to operate as a Layer 2 interface.

This command does not require a license.

Examples

This example shows how to configure the aging type to be “inactivity” on the Ethernet 2/1 interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security aging type inactivity
switch(config-if)#
```

Related Commands

Command	Description
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security	Configures a Layer 2 interface for port security.
switchport port-security aging time	Configures the aging time for dynamically learned, secure MAC addresses.
switchport port-security mac-address	Configures a static MAC address.
switchport port-security mac-address sticky	Enables the sticky method for learning secure MAC addresses.
switchport port-security maximum	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
switchport port-security violation	Configures the security violation action for an interface.

switchport port-security mac-address

To configure a static, secure MAC address on an interface, use the **switchport port-security mac-address** command. To remove a static, secure MAC address from an interface, use the **no** form of this command.

switchport port-security mac-address *address* [**vlan** *vlan-ID*]

no switchport port-security mac-address *address* [**vlan** *vlan-ID*]

Syntax Description

address	MAC address that you want to specify as a static, secure MAC address on the current interface.
vlan *vlan-ID*	(Optional) Specifies the VLAN on which traffic from the MAC address is permitted. Valid VLAN IDs are from 1 to 4096.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

There are no default static, secure MAC addresses.

You must enable port security by using the **feature port-security** command before you can use the **switchport port-security mac-address** command.

Before using this command, you must use the **switchport** command to configure the interface to operate as a Layer 2 interface.

This command does not require a license.

Examples

This example shows how to configure 0019.D2D0.00AE as a static, secure MAC address on the Ethernet 2/1 interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE
switch(config-if)#
```

Related Commands

Command	Description
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security	Configures a Layer 2 interface for port security.
switchport port-security aging time	Configures the aging time for dynamically learned, secure MAC addresses.
switchport port-security aging type	Configures the aging type for dynamically learned, secure MAC addresses.
switchport port-security mac-address sticky	Enables the sticky method for learning secure MAC addresses.
switchport port-security maximum	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
switchport port-security violation	Configures the security violation action for an interface.

switchport port-security mac-address sticky

To enable the sticky method for learning secure MAC addresses on a Layer 2 Ethernet interface or Layer 2 port-channel interface, use the **switchport port-security mac-address sticky** command. To disable the sticky method and return to the dynamic method, use the **no** form of this command.

switchport port-security mac-address sticky

no switchport port-security mac-address sticky

Syntax Description

This command has no arguments or keywords.

Command Default

The sticky method of secure MAC address learning is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

You must enable port security by using the **feature port-security** command before you can use the **switchport port-security mac-address sticky** command.

Before using this command, you must use the **switchport** command to configure the interface to operate as a Layer 2 interface.

This command does not require a license.

Examples

This example shows how to enable the sticky method of learning secure MAC addresses on the Ethernet 2/1 interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security mac-address sticky
switch(config-if)#
```

Related Commands

Command	Description
feature port-security	Enables port security globally.
show port-security	Shows information about port security.

Command	Description
switchport port-security	Enables port security on a Layer 2 interface.
switchport port-security aging time	Configures the aging time for dynamically learned, secure MAC addresses.
switchport port-security aging type	Configures the aging type for dynamically learned, secure MAC addresses.
switchport port-security mac-address	Configures a static MAC address.
switchport port-security maximum	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
switchport port-security violation	Configures the security violation action for an interface.

switchport port-security maximum

To configure the interface maximum or a VLAN maximum of secure MAC addresses on a Layer 2 Ethernet interface or Layer 2 port-channel interface, use the **switchport port-security maximum** command. To remove port security configuration, use the **no** form of this command.

switchport port-security maximum *number* [**vlan** *vlan-ID*]

no switchport port-security maximum *number* [**vlan** *vlan-ID*]

Syntax Description

maximum *number*	Specifies the maximum number of secure MAC addresses. See the "Usage Guidelines" section for information about valid values for the *number* argument.
vlan *vlan-ID*	(Optional) Specifies the VLAN that the maximum applies to. If you omit the **vlan** keyword, the maximum is applied as an interface maximum.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

The default interface maximum is one secure MAC address.

Enabling port security on an interface also enables the default method for learning secure MAC addresses, which is the dynamic method. To enable the sticky learning method, use the **switchport port-security mac-address sticky** command.

You must enable port security by using the **feature port-security** command before you can use the **switchport port-security maximum** command.

Before using this command, you must use the **switchport** command to configure the interface to operate as a Layer 2 interface.

There is no default VLAN maximum.

There is a system-wide, nonconfigurable maximum of 4096 secure MAC addresses.

This command does not require a license.

Maximums for Access Ports and Trunk Ports

For an interface used as an access port, we recommend that you use the default interface maximum of one secure MAC address.

For an interface used as a trunk port, set the interface maximum to a number that reflects the actual number of hosts that could use the interface.

Interface Maximums, VLAN Maximums, and the Device Maximum

The sum of all VLAN maximums that you configure on an interface cannot exceed the interface maximum. For example, if you configure a trunk-port interface with an interface maximum of 10 secure MAC addresses and a VLAN maximum of 5 secure MAC addresses for VLAN 1, the largest maximum number of secure MAC addresses that you can configure for VLAN 2 is also 5. If you tried to configure a maximum of 6 secure MAC addresses for VLAN 2, the device would not accept the command.

Examples

This example shows how to configure an interface maximum of 10 secure MAC addresses on the Ethernet 2/1 interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security maximum 10
switch(config-if)#
```

Related Commands

Command	Description
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security	Enables port security on a Layer 2 interface.
switchport port-security aging time	Configures the aging time for dynamically learned, secure MAC addresses.
switchport port-security aging type	Configures the aging type for dynamically learned, secure MAC addresses.
switchport port-security mac-address	Configures a static MAC address.
switchport port-security mac-address sticky	Enables the sticky method for learning secure MAC addresses.
switchport port-security violation	Configures the security violation action for an interface.

switchport port-security violation

To configure the action that the device takes when a security violation event occurs on an interface, use the **switchport port-security violation** command. To remove the port security violation action configuration, use the **no** form of this command.

switchport port-security violation {**protect**| **restrict**| **shutdown**}

no switchport port-security violation {**protect**| **restrict**| **shutdown**}

Syntax Description

protect	Specifies that the device does not raise security violations when a packet would normally trigger a security violation event. Instead, the address that triggered the security violation is learned but any traffic from the address is dropped. Further address learning stops.
restrict	Specifies that the device drops ingress traffic from any nonsecure MAC addresses. Address learning continues until 100 security violations have occurred on the interface. Traffic from addresses learned after the first security violation is dropped. After 100 security violations occur, the device disables learning on the interface and drops all ingress traffic from nonsecure MAC addresses. In addition, the device generates an SNMP trap for each security violation.
shutdown	Specifies that the device shuts down the interface if it receives a packet triggering a security violation. The interface is error disabled. This action is the default. After you reenable the interface, it retains its port security configuration, including its secure MAC addresses.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

The default security violation action is to shut down the interface.

You must enable port security by using the **feature port-security** command before you can use the **switchport port-security violation** command.

Before using this command, you must use the **switchport** command to configure the interface to operate as a Layer 2 interface.

Port security triggers security violations when either of the two following events occur:

- Ingress traffic arrives at an interface from a nonsecure MAC address and learning the address would exceed the applicable maximum number of secure MAC addresses.

When an interface has both a VLAN maximum and an interface maximum configured, a violation occurs when either maximum is exceeded. For example, consider the following on a single interface configured with port security:

-
  - VLAN 1 has a maximum of 5 addresses
  - The interface has a maximum of 10 addresses

The device detects a violation when any of the following occurs:

-
  - The device has learned five addresses for VLAN 1 and inbound traffic from a sixth address arrives at the interface in VLAN 1.
  - The device has learned 10 addresses on the interface and inbound traffic from an 11th address arrives at the interface.

- Ingress traffic from a secure MAC address arrives at a different interface in the same VLAN as the interface on which the address is secured.

Note After a secure MAC address is configured or learned on one secure port, the sequence of events that occurs when port security detects that secure MAC address on a different port in the same VLAN is known as a MAC move violation.

When a security violation occurs, the device takes the action specified by the port security configuration of the applicable interface. The possible actions are as follows:

- Shutdown—Shuts down the interface that received the packet triggering the violation. The interface is error disabled. This action is the default. After you reenable the interface, it retains its port security configuration, including its secure MAC addresses.

You can use the **errdisable** global configuration command to configure the device to reenable the interface automatically if a shutdown occurs, or you can manually reenable the interface by entering the **shutdown** and **no shut down** interface configuration commands.

- Restrict—Drops ingress traffic from any nonsecure MAC addresses. Address learning continues until 100 security violations have occurred on the interface. Traffic from addresses learned after the first security violation is dropped.

After 100 security violations occur, the device disables learning on the interface and drops all ingress traffic from nonsecure MAC addresses. In addition, the device generates an SNMP trap for each security violation.

- Protect—Prevents further violations from occurring. The address that triggered the security violation is learned but any traffic from the address is dropped. Further address learning stops.

If a violation occurs because ingress traffic from a secure MAC address arrives at a different interface than the interface on which the address is secure, the device applies the action on the interface that received the traffic.

This command does not require a license.

Examples

This example shows how to configure an interface to respond to a security violation event with the protect action:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security violation protect
switch(config-if)#
```

Related Commands

Command	Description
feature port-security	Enables port security globally.
show port-security	Shows information about port security.
switchport port-security	Enables port security on a Layer 2 interface.
switchport port-security aging time	Configures the aging time for dynamically learned, secure MAC addresses.
switchport port-security aging type	Configures the aging type for dynamically learned, secure MAC addresses.
switchport port-security mac-address	Configures a static MAC address.
switchport port-security mac-address sticky	Enables the sticky method for learning secure MAC addresses.
switchport port-security maximum	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.

Show Commands

show

To display information about which I/O modules are configured with the command, use the **show** command.

show

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

If no I/O modules are configured with the command, the **show** command has no output.

Examples

This example shows how to display the I/O modules that are configured with the command:

```
switch# show
  Module 1 enabled
  Module 3 enabled
switch#
```

show aaa accounting

To display AAA accounting configuration information, use the **show aaa accounting** command.

show aaa accounting

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the configuration of the accounting log:

```
switch# show aaa accounting
         default: local
```

show aaa authentication

To display AAA authentication configuration information, use the **show aaa authentication** command.

show aaa authentication [**login error-enable**| **login chap**| **login mschap**| **login mschapv2**| **login ascii-authentication**]

Syntax Description

login error-enable	(Optional) Displays the configuration for login error messages.
login chap	(Optional) Displays the configuration for CHAP authentication.
login mschap	(Optional) Displays the configuration for MS-CHAP authentication.
login mschapv2	(Optional) Displays the configuration for MS-CHAP V2 authentication.
login ascii-authentication	(Optional) Displays the configuration for ASCII authentication for passwords on TACACS+ servers.

Command Default

Displays the console and login authentication methods configuration.

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	Added the **chap** keyword
4.2(1)	Added the **mschapv2** keyword.
4.1(2)	Added the **ascii-authentication** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the configured authentication parameters:

```
switch# show aaa authentication
         default: local
         console: local
         dot1x: not configured
         eou: not configured
```

This example shows how to display the authentication-login error-enable configuration:

```
switch# show aaa authentication login error-enable
disabled
```

This example shows how to display the authentication-login CHAP configuration:

```
switch# show aaa authentication login chap
disabled
```

This example shows how to display the authentication-login MSCHAP configuration:

```
switch# show aaa authentication login mschap
disabled
```

This example shows how to display the authentication-login MSCHAP V2 configuration:

```
switch# show aaa authentication login mschapv2
enabled
```

This example shows how to display the status of the ASCII authentication for passwords feature :

```
switch(config)# show aaa authentication login ascii-authentication
disabled
```

Related Commands

Command	Description
aaa authentication login ascii-authentication	Enables ASCII authentication for passwords on a TACACS+ server.
aaa authentication login chap enable	Enables CHAP authentication.
aaa authentication login error-enable	Configures the AAA authentication failure message to display on the console.
aaa authentication login mschap enable	Enables MSCHAP authentication.
aaa authentication login mschapv2 enable	Enables MSCHAP V2 authentication.

show aaa authorization

To display AAA authorization configuration information, use the **show aaa authorization** command.

show aaa authorization [all]

Syntax Description

all	(Optional) Displays configured and default values.

Command Default

Displays the configured information.

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the configured authorization methods:

```
switch# show aaa authorization
   pki-ssh-cert: local
         pki-ssh-pubkey: local
AAA command authorization:
         default authorization for config-commands: none
         cts: group radius
```

This example shows how to display the configured authorization methods and defaults:

```
switch# show aaa authorization all
   pki-ssh-cert: local
         pki-ssh-pubkey: local
AAA command authorization:
         default authorization for config-commands: none
         default authorization for commands: local
         cts: group radius
```

Related Commands

Command	Description
aaa authorization	Configures the default AAA authorization method.
feature cts	Enables the Cisco TrustSec feature.

Command	Description
feature ldap	Enables the LDAP feature.
feature tacacs+	Enables the TACACS+ feature.

show aaa groups

To display AAA server group configuration, use the **show aaa groups** command.

show aaa groups

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display AAA group information:

```
switch# show aaa groups
radius
TacServer
```

show aaa local user blocked

To display the blocked users, use the **show aaa local user blocked** command.

show aaa local user blocked

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the blocked users:

```
switch# show aaa local user blocked
Local-user       State
testuser         Watched (till 11:34:42 IST Feb 5 2015)
```

Related Commands

Command	Description
aaa authentication rejected	Configures the login block per user.
clear aaa local user blocked	Clears the blocked users.

show aaa user default-role

To display the AAA user default role configuration, use the **show aaa user default-role** command.

show aaa user default-role

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

User the **aaa user default-role** command to configure the AAA user default role.

This command does not require a license.

Examples

This example shows how to display the AAA user default role configuration:

```
switch# show aaa user default-role
enabled
```

Related Commands

Command	Description
aaa user default-role	Enables the AAA user default role.

show access-list status module

To display the access control list (ACL) capture configuration, use the show access-list status module command.

show access-list status module *slot*

Syntax Description

slot	Slot ID. The range is from 1 to 18.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the access control list (ACL) capture configuration:

```
switch(config)# show access-list status module 5
Non-Atomic ACL updates Disabled.
TCAM Default Result is Deny.
Resource-pooling: Disabled
switch(config)#
```

Related Commands

Command	Description
access-list capture	Enables access control list (ACL) capture on all virtual device contexts (VDCs).

show access-lists

To display all IPv4, IPv6, and MAC access control lists (ACLs) or a specific ACL, use the **show access-lists** command.

show access-lists [*access-list-name*] [**expanded| summary**]

Syntax Description

access-list-name	(Optional) Name of an ACL, which can be up to 64 alphanumeric, case-sensitive characters.
expanded	(Optional) Specifies that the contents of object groups appear rather than the names of object groups only.
summary	(Optional) Specifies that the command displays information about the ACL. For more information, see the “Usage Guidelines” section.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names. Support was added for the **fragments** command.
4.1(2)	Support for IPv6 ACLs was added.
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all ACLs unless you use the *access-list-name* argument to specify an ACL.

If you do not specify an ACL name, the device lists ACLs alphabetically by the ACL names.

The **expanded** keyword allows you to display the details of object groups used in an ACL rather than only the name of the object groups. For more information about object groups, see the **object-group ip address**, **object-group ipv6 address**, and **object-group ip port** commands.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics are configured for the ACL.

- Whether the **fragments** command is configured for an IP ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries that the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

If an IP ACL includes the **fragments** command, it appears before the explicit permit and deny rules, but the device applies the **fragments** command to noninitial fragments only if they do not match all other explicit rules in the ACL.

This command does not require a license.

Examples

This example shows how to use the **show access-lists** command without specifying an ACL name on a device that has one IP ACL and one MAC ACL configured:

```
switch# show access-lists
IP access list ip-v4-filter
        10 permit ip any any
MAC access list mac-filter
        10 permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff ip
```

This example shows how to use the **show access-lists** command to display an IPv4 ACL named ipv4-RandD-outbound-web, including per-entry statistics for the entries except for the MainLab object group:

```
switch# show access-lists ipv4-RandD-outbound-web
IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp addrgroup MainLab any eq telnet
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show access-lists** command to display an IPv4 ACL named ipv4-RandD-outbound-web. The **expanded** keyword causes the contents of the object group from the previous example to appear, including the per-entry statistics:

```
switch# show access-lists ipv4-RandD-outbound-web expanded
IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp 10.52.34.4/32 any eq telnet [match=5032]
        1005 permit tcp 10.52.34.27/32 any eq telnet [match=433]
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show access-lists** command with the **summary** keyword to display information about an IPv4 ACL named ipv4-RandD-outbound-web, such as which interfaces the ACL is applied to and active on:

```
switch# show access-lists ipv4-RandD-outbound-web summary
IPV4 ACL ipv4-RandD-outbound-web
        Statistics enabled
        Total ACEs Configured: 4
```

```
Configured on interfaces:
        Ethernet2/4 - ingress (Router ACL)
Active on interfaces:
        Ethernet2/4 - ingress (Router ACL)
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ip access-list	Configures an IPv4 ACL.
ipv6 access-list	Configures an IPv6 ACL.
mac access-list	Configures a MAC ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show ipv6 access-lists	Displays all IPv6 ACLs or a specific IPv6 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

show accounting log

To display the accounting log contents, use the **show accounting log** command.

show accounting log [*size*| **last-index**| **start-seqnum** *number*| **start-time** *year month day HH* **:** *MM* **:** *SS*]

Syntax Description

size	(Optional) Size of the log to display in bytes. The range is from 0 to 250000.
last-index *number*	(Optional) Displays the last index number in the log.
start-seqnum	(Optional) Specifies a sequence number in the log at which to begin display output. The range is from 1 to 1000000.
start-time*year month day HH*:*MM*:*SS*	(Optional) Specifies a start time in the log at which to begin displaying output. The *year* argument is in *yyyy* format. The *month* is the three-letter English abbreviation. The *day* argument range is from 1 to 31. The *HH*:*MM*:*SS* argument is in the standard 24-hour format.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Added the **last-index** and **start-seqnum** keyword options.
4.0(1)	This command was introduced.

Usage Guidelines

When you make a change to the configuration, the results are shown in the output for **show accounting log**. There three results for the configuration change:

- **Success**: indicates the configuration change was successful.
- **Failure**: indicates the configuration change was unsuccessful.

- **Redirect**: indicates the configuration change was not issued directly from the Command Line Interface (CLI) but was issued as a result of another CLI command. For example, the following output is issued as a result of the **port-profile type** command:

```
Fri Sep 27 16:15:08 2013:type=update:id=console0:user=admin:cmd=switchto ; configure terminal
 ; port-profile type port-channel GANETTI-OKEANOS ; switchport trunk allowed vlan add 71
(REDIRECT)
```

This command does not require a license.

Examples

This example shows how to display the entire accounting log:

```
switch# show accounting log
Sat Feb 16 10:44:24 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 10:44:25 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 10:45:20 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log
file start-time 2008 Feb 16 10:44:11
Sat Feb 16 10:45:23 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting
log start-time 2008 Feb 16 10:08:57
Sat Feb 16 10:45:24 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 10:45:25 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 10:46:20 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log
file start-time 2008 Feb 16 10:45:11
Sat Feb 16 10:46:22 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting
```

This example shows how to display 400 bytes of the accounting log:

```
switch# show accounting log 400
Sat Feb 16 21:15:24 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log start-time
 2008 Feb 16 18:31:21
Sat Feb 16 21:15:25 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 21:15:26 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
```

This example shows how to display the accounting log starting at 16:00:00 on February 16, 2008:

```
switch(config)# show accounting log start-time 2008 Feb 16 16:00:00
Sat Feb 16 16:00:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 15:59:16
Sat Feb 16 16:00:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log start-time
 2008 Feb 16 12:05:16
Sat Feb 16 16:00:27 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 16:00:28 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 16:01:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 16:00:16
Sat Feb 16 16:01:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log start-time
 2008 Feb 16 12:05:16
Sat Feb 16 16:01:27 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 16:01:29 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 16:02:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 16:01:16
Sat Feb 16 16:02:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log start-time
 2008 Feb 16 12:05:16
Sat Feb 16 16:02:28 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
```

This example shows how to display the last index number:

```
switch# show accounting log last-index
accounting-log last-index : 1814
```

This example shows how to display the result of configuration changes:

```
switch# show accounting log
Fri Mar 15 10:19:58 2013:type=update:id=console0:user=Ciscoadmin:cmd=configure terminal ;
interface Ethernet1/1 (SUCCESS)
Fri Mar 15 10:19:59 2013:type=update:id=console0:user=Ciscoadmin:cmd=configure terminal ;
interface Ethernet1/1 ; shutdown (REDIRECT)
Fri Mar 15 10:19:59 2013:type=update:id=console0:user=Ciscoadmin:cmd=configure terminal ;
interface Ethernet1/1 ; shutdown (SUCCESS)
```

```
Fri Mar 15 10:20:03 2013:type=update:id=console0:user=Ciscoadmin:cmd=configure terminal ;
interface Ethernet1/1 ; no shutdown (REDIRECT)
Fri Mar 15 10:20:03 2013:type=update:id=console0:user=Ciscoadmin:cmd=configure terminal ;
interface Ethernet1/1 ; no shutdown (SUCCESS)
```

Related Commands

Command	Description
clear accounting log	Clears the accounting log.

show arp access-lists

To display all ARP access control lists (ACLs) or a specific ARP ACL, use the **show arp access-lists** command.

show arp access-lists [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of an ARP ACL, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all ARP ACLs, unless you use the *access-list-name* argument to specify an ACL.

This command does not require a license.

Examples

This example shows how to use the **show arp access-lists** command to display all ARP ACLs on a device that has two ARP ACLs:

```
switch# show arp access-lists
ARP access list arp-permit-all
10 permit ip any mac any
ARP access list arp-lab-subnet
10 permit request ip 10.32.143.0 255.255.255.0 mac any
```

This example shows how to use the **show arp access-lists** command to display an ARP ACL named arp-permit-all:

```
switch# show arp access-lists arp-permit-all
ARP access list arp-permit-all
10 permit ip any mac any
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip arp inspection filter	Applies an ARP ACL to a VLAN.

show class-map type control-plane

To display control plane class map information, use the **show class-map type control-plane** command.

show class-map type control-plane [*class-map-name*]

Syntax Description

class-map-name	(Optional) Name of the control plane class map.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display control plane class map information:

```
switch# show class-map type control-plane
    class-map type control-plane match-any copp-system-class-critical
      match access-grp name copp-system-acl-arp
      match access-grp name copp-system-acl-msdp
    class-map type control-plane match-any copp-system-class-important
      match access-grp name copp-system-acl-gre
      match access-grp name copp-system-acl-tacas
    class-map type control-plane match-any copp-system-class-normal
      match access-grp name copp-system-acl-icmp
      match redirect dhcp-snoop
      match redirect arp-inspect
      match exception ip option
      match exception ip icmp redirect
      match exception ip icmp unreachable
```

show cli syntax roles network-admin

To display the syntax of the commands that the network-admin role can use but the vdc-admin role cannot, use the **show cli syntax roles network-admin** command.

show cli syntax roles network-admin

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the syntax of the commands that the network-admin role can use but the vdc-admin role cannot:

```
switch# show cli syntax roles network-admin
MODE exec
(0) show debug license
(1) show debug bootvar
(2) show debug cmpproxy
(3) show debug exceptionlog
(4) show debug device_test
(5) show debug diagmgr
(6) show debug diagclient
(7) show debug ntp
(8) show debug port_lb
(9) show debug copp
(10) show debug copp bypass
(11) show license usage vdc-all [ { detail | <license-feature> } ]
(12) show system internal license event-history
(13) show system internal license mem-stats [ detail ]
(14) show system internal loader configuration
(15) show system internal bootvar log
(16) show system internal cmpproxy install-logs
(17) show system internal cmpproxy [ event-history ] errors
(18) show system internal cmpproxy [ event-history ] msgs
(19) show system internal cmpproxy mem-stats [ detail ]
(20) show system internal epld logging
(21) c status [ ]
(22) show system internal copp ppf-database { policy { subscriptions | sessions
| instances | all } }
(23) show system internal copp [ event-history ] errors
(24) show system internal copp [ event-history ] logs
(25) show system internal copp [ event-history ] msgs
```

```
(26) show system internal copp mem-stats [ detail ]
(27)  show system internal copp info
(28) show system reset-reason
(29) show system reset-reason module <module>
(30) show system reset-reason <s0> <santa-cruz-range>
(31) show system redundancy status
(32) show system redundancy ha status
(33) show logging level { license | licmgr }
(34) show logging level bootvar
(35) show logging level cmpproxy
(36) show logging level diagnostic device_test
(37) show logging level diagnostic diagmgr
(38) show logging level diagnostic diagclient
(39) show logging level ntp
(40) show logging level copp
(41) show running-config res_mgr
(42) show running-config vdc [ all ]
(43) show running-config diagnostic [ all ]
(44) show running-config cmp
(45) show running-config ntp [ all ]
(46) show running-config vdc-all [ all ]
(47) show running-config copp [ all ]
(48) show startup-config vdc [ all ]
(49) show startup-config diagnostic [ all ]
(50) show startup-config ntp [ all ]
(51) show startup-config vdc-all
(52) show startup-config copp [ all ]
(53) show tech-support gold
(54) show tech-support cmp
(55) show tech-support dcbx
(56) show tech-support ntp
(57) show tech-support forwarding l2 multicast vdc-all
(58) show tech-support forwarding l3 unicast vdc-all [ module <module> ]
--More--
```

Related Commands

Command	Description
show cli syntax roles network-operator	Displays the syntax of the commands that the network-operator role can use but the vdc-operator role cannot.

show cli syntax roles network-operator

To display the syntax of the commands that the network-operator role can use but the vdc-operator role cannot, use the **show cli syntax roles network-operator** command.

show cli syntax roles network-operator

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the syntax of the commands that the network-operator role can use but the vdc-operator role cannot:

```
switch# show cli syntax roles network-operator
MODE exec
(0) show debug license
(1) show debug cmpproxy
(2) show debug exceptionlog
(3) show debug device_test
(4) show debug diagmgr
(5) show debug diagclient
(6) show debug ntp
(7) show debug port_lb
(8) show debug copp
(9) show license usage vdc-all [ { detail | <license-feature> } ]
(10) show system internal license event-history
(11) show system internal license mem-stats [ detail ]
(12) show system internal loader configuration
(13) show system internal bootvar log
(14) show system internal cmpproxy install-logs
(15) show system internal cmpproxy [ event-history ] errors
(16) show system internal cmpproxy [ event-history ] msgs
(17) show system internal cmpproxy mem-stats [ detail ]
(18) show system internal epld logging
(19) show system internal access-list status [ ]
(20) show system internal copp ppf-database { policy { subscriptions | sessions
| instances | all } }
(21) show system internal copp [ event-history ] errors
--More--
```

Related Commands

Command	Description
show cli syntax roles network-admin	Displays the syntax of the commands that the network-admin role can use but the vdc-admin role cannot.

show copp diff profile

To display the difference between the previous and latest Control Plane Policing (CoPP) best practice policies or between the currently applied default CoPP best practice policy and the latest CoPP best practice policy, use the **show copp diff profile** command.

show copp diff profile {**lenient**| **moderate**| **strict**} **[prior-ver] profile** {**lenient**| **moderate**| **strict**}

Syntax Description

lenient	Displays the lenient profile.
moderate	Displays the moderate profile.
strict	Displays the strict profile.
profile	Specifies the profile.
prior-ver	Specifies the previous profile.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

When you do not include the **prior-ver** option, this command displays the difference between two currently applied default CoPP best practice policies (such as the currently applied strict and currently applied moderate policies).

When you include the **prior-ver** option, this command displays the difference between a currently applied default CoPP best practice policy and a previously applied default CoPP best practice policy (such as the currently applied strict and the previously applied lenient policies).

This command does not require a license.

Examples

This example shows how to display the difference between the currently applied default CoPP best practice policy and the latest CoPP best practice policy:

```
switch# show copp diff profile moderate applied latest
```

Related Commands

Command	Description
show copp profile	Displays the details of the CoPP best practice policy, along with the classes and policer values.

show copp profile

To display the details of the Control Plane Policing (CoPP) best practice policy, along with the classes and policer values, use the **show copp profile** command.

show copp profile {**lenient**| **moderate**| **strict**}

Syntax Description

lenient	Displays the lenient profile.
moderate	Displays the moderate profile.
strict	Displays the strict profile.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the details of the CoPP best practice policy, along with the classes and policer values:

```
switch# show copp profile moderate
ip access-list copp-system-p-acl-bgp
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-p-acl-bgp6
  permit tcp any gt 1024 any eq bgp
  permit tcp any eq bgp any gt 1024
ip access-list copp-system-p-acl-cts
  permit tcp any any eq 64999
  permit tcp any eq 64999 any
ip access-list copp-system-p-acl-dhcp
  permit udp any eq bootpc any
  permit udp any neq bootps any eq bootps
ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
  permit udp any any eq bootpc
ip access-list copp-system-p-acl-eigrp
  permit eigrp any any
ip access-list copp-system-p-acl-ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq ftp
  permit tcp any eq ftp-data any
  permit tcp any eq ftp any
ip access-list copp-system-p-acl-glbp
  permit udp any eq 3222 224.0.0.0/24 eq 3222
--More--
```

Related Commands

Command	Description
copp profile	
copp clone profile	
show copp diff profile	Displays the difference between the currently applied default CoPP best practice policy and the latest or previous CoPP best practice policy.
show copp status	Displays the CoPP status, including the last configuration operation and its status.
show running-config copp	Displays the CoPP configuration in the running configuration.

show copp status

To display the control plane policing (CoPP) configuration status, use the **show copp status** command.

show copp status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(2)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display the CoPP configuration status information:

```
switch# show copp status
Last Config Operation: service-policy input copp-system-policy
Last Config Operation Timestamp: 21:57:58 UTC Jun  4 2008
Last Config Operation Status: Success
Policy-map attached to the control-plane: new-copp-policy
```

show crypto ca certificates

To display configured trustpoint certificates, use the **show crypto ca certificates** command.

show crypto ca certificates *trustpoint-label*

Syntax Description

trustpoint-label	Name of the trustpoint. The name is case sensitive.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use this command to display the fields in the identity certificate, if present, followed by the fields in the CA certificate (or each CA certificate if it is a chain, starting from the lowest to the self-signed root certificate), or the trustpoint. If the trustpoint name is not specified, all trustpoint certificate details are displayed.

This command does not require a license.

Examples

This example shows how to display configured trustpoint certificates:

```
switch# show crypto ca certificates
Trustpoint: admin-ca
certificate:
subject= /CN=switch160
issuer= /C=US/O=cisco/CN=Aparna CA2
serial=6CDB2D9E000100000006
notBefore=Jun  9 10:51:45 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=0A:22:DC:A3:07:2A:9F:9A:C2:2C:BA:96:EC:D8:0A:95
purposes: sslserver sslclient ike
CA certificate 0:
subject= /C=US/O=cisco/CN=Aparna CA2
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Maharashtra/L=Pune/O=cisco/OU=ne
tstorage/CN=Aparna CA1
serial=14A3A877000000000005
notBefore=May  5 18:43:36 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=32:50:26:9B:16:B1:40:A5:D0:09:53:0A:98:6C:14:CC
purposes: sslserver sslclient ike
CA certificate 1:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Maharashtra/L=Pune/O=cisco/OU=n
etstorage/CN=Aparna CA1
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
```

```
serial=611B09A1000000000002
notBefore=May  3 23:00:36 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=65:CE:DA:75:0A:AD:B2:ED:69:93:EF:5B:58:D4:E7:AD
purposes: sslserver sslclient ike
CA certificate 2:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/O
U=netstorage/CN=Aparna CA
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the CA.
show ca trustpoints	Displays trustpoint configurations.

show crypto ca certstore

To display the cert-store configuration, use the **show crypto ca certstore** command.

show crypto ca certstore

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

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 display the cert-store configuration:

```
switch# show crypto ca certstore
Certstore lookup: REMOTE
```

Related Commands

Command	Description
crypto ca lookup	Specifies the cert-store to be used for certificate authentication.
show crypto ca remote-certstore	Displays the remote cert-store configuration.

show crypto ca crl

To display configured certificate revocation lists (CRLs), use the **show crypto ca crl** command.

show crypto ca crl trustpoint-label

Syntax Description

trustpoint-label	Name of the trustpoint. The label is case sensitive.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Use this command to list the serial numbers of the revoked certificates in the CRL of the specified trustpoint.

This command does not require a license.

Examples

This example shows how to display a configured CRL:

```
switch# show crypto ca crl admin-ca
Trustpoint: admin-ca
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /emailAddress=rviyyoka@cisco.com/C=IN/ST=Kar/L=Bangalore/O=Cisco
 Systems/OU=1/CN=cisco-blr
        Last Update: Sep 22 07:05:23 2005 GMT
        Next Update: Sep 29 19:25:23 2005 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:CF:72:E1:FE:14:60:14:6E:B0:FA:8D:87:18:6B:E8:5F:70:69:05:3F
            1.3.6.1.4.1.311.21.1:
                ...
Revoked Certificates:
    Serial Number: 1E0AE838000000000002
        Revocation Date: Mar 15 09:12:36 2005 GMT
    Serial Number: 1E0AE9AB000000000003
        Revocation Date: Mar 15 09:12:45 2005 GMT
    Serial Number: 1E721E50000000000004
        Revocation Date: Apr  5 11:04:20 2005 GMT
    Serial Number: 3D26E445000000000005
        Revocation Date: Apr  5 11:04:16 2005 GMT
    Serial Number: 3D28F8DF000000000006
        Revocation Date: Apr  5 11:04:12 2005 GMT
```

```
Serial Number: 3D2C6EF3000000000007
    Revocation Date: Apr  5 11:04:09 2005 GMT
Serial Number: 3D4D7DDC000000000008
    Revocation Date: Apr  5 11:04:05 2005 GMT
Serial Number: 5BF1FE87000000000009
    Revocation Date: Apr  5 11:04:01 2005 GMT
Serial Number: 5BF22FB300000000000A
    Revocation Date: Apr  5 11:03:45 2005 GMT
Serial Number: 5BFA4A4900000000000B
    Revocation Date: Apr  5 11:03:42 2005 GMT
Serial Number: 5C0BC22500000000000C
    Revocation Date: Apr  5 11:03:39 2005 GMT
Serial Number: 5C0DA95E00000000000D
    Revocation Date: Apr  5 11:03:35 2005 GMT
Serial Number: 5C13776900000000000E
    Revocation Date: Apr  5 11:03:31 2005 GMT
Serial Number: 4864FD5A00000000000F
    Revocation Date: Apr  5 11:03:28 2005 GMT
Serial Number: 48642E2E000000000010
    Revocation Date: Apr  5 11:03:24 2005 GMT
Serial Number: 486D4230000000000011
    Revocation Date: Apr  5 11:03:20 2005 GMT
Serial Number: 7FCB75B9000000000012
    Revocation Date: Apr  5 10:39:12 2005 GMT
Serial Number: 1A7519000000000013
    Revocation Date: Apr  5 10:38:52 2005 GMT
Serial Number: 20F1B0000000000014
    Revocation Date: Apr  5 10:38:38 2005 GMT
Serial Number: 436E43A9000000000023
    Revocation Date: Sep  9 09:01:23 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 152D3C5E000000000047
    Revocation Date: Sep 22 07:12:41 2005 GMT
Serial Number: 1533AD7F000000000048
    Revocation Date: Sep 22 07:13:11 2005 GMT
Serial Number: 1F9EB8EA00000000006D
    Revocation Date: Jul 19 09:58:45 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 1FCA9DC600000000006E
    Revocation Date: Jul 19 10:17:34 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 2F1B5E2E000000000072
    Revocation Date: Jul 22 09:41:21 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Signature Algorithm: sha1WithRSAEncryption
    4e:3b:4e:7a:55:6b:f2:ec:72:29:70:16:2a:fd:d9:9a:9b:12:
    f9:cd:dd:20:cc:e0:89:30:3b:4f:00:4b:88:03:2d:80:4e:22:
    9f:46:a5:41:25:f4:a5:26:b7:b6:db:27:a9:64:67:b9:c0:88:
    30:37:cf:74:57:7a:45:5f:5e:d0
```

Related Commands

Command	Description
crypto ca crl request	Configures a CRL or overwrites the existing one for the trustpoint CA.

show crypto ca remote-certstore

To display the remote cert-store configuration, use the **show crypto ca remote-certstore** command.

show crypto ca remote-certstore

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

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 display the remote cert-store configuration:

```
switch# show crypto ca remote-certstore
Remote Certstore: NONE
```

Related Commands

Command	Description
crypto ca lookup	Specifies the cert-store to be used for certificate authentication.
show crypto ca certstore	Displays the configured cert-store.

show crypto ca trustpoints

To display trustpoint configurations, use the **show crypto ca trustpoints** command.

show crypto ca trustpoints

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

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 display configured trustpoints:

```
switch# show crypto ca trustpoints
trustpoint: CAname; key:
revokation methods:  crl
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the CA.
crypto ca trustpoint	Declares the trustpoint certificate authority that the device should trust.
show crypto ca certificates	Displays configured trustpoint certificates.

show crypto certificatemap

To display the certificate mapping filters, use the **show crypto certificatemap** command.

show crypto certificatemap

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

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 display the certificate mapping filters:

```
switch# show crypto certificatemap
```

Related Commands

Command	Description
crypto certificatemap mapname	Creates a filter map.
filter	Configures one or more certificate mapping filters within the filter map.

show crypto key mypubkey rsa

To display the RSA public key configurations, use the **show crypto key mypubkey rsa** command.

show crypto key mypubkey rsa

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

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 display RSA public key configurations:

```
switch# show crypto key mypubkey rsa
key label: myrsa
key size: 512
exportable: yes
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch’s RSA key pair.
crypto key generate rsa	Generate an RSA key pair.
rsakeypair	Configure trustpoint RSA key pair details

show crypto ssh-auth-map

To display the mapping filters configured for SSH authentication, use the ssh-auth-map**showcrypto ssh-auth-map**command.

show crypto ssh-auth-map

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

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 display the mapping filters configured for SSH authentication:

```
switch# show crypto ssh-auth-map
Default Map     : filtermap1
```

Related Commands

Command	Description
crypto certificatemap mapname	Creates a filter map.
crypto cert ssh-authorize	Configures a certificate mapping filter for the SSH protocol.
filter	Configures one or more certificate mapping filters within the filter map.

show cts

To display the global Cisco TrustSec configuration, use the **show cts** command.

show cts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec global configuration:

```
switch# show cts
CTS Global Configuration
==============================
  CTS support           : enabled
  CTS device identity   : Device1
  CTS caching support   : disabled
  Number of CTS interfaces in
    DOT1X mode : 0
    Manual mode : 0
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts capability interface

To display the Cisco TrustSec capability of all interfaces or a specific Ethernet interface, use the show cts capability interface command.

show cts capability interface {**all**| **ethernet**}

Syntax Description

all	Displays the Cisco TrustSec capability of all interfaces.
ethernet slot/port	Displays the Cisco TrustSec capability of the specific interface.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec capability of all interfaces:

```
switch# show cts capability interface all
CTS capability information for interface(s)
--------- --- ------ ---------------------------------------
Interface SGT MacSec Comments
--------- --- ------ ---------------------------------------
Eth6/1    Yes Yes    cts dot1x and manual configs allowed
Eth8/1    Yes Yes    cts dot1x and manual configs allowed
Eth8/17   Yes Yes    cts dot1x and manual configs allowed
Eth8/33   Yes Yes    cts dot1x and manual configs allowed
Eth6/2    Yes Yes    cts dot1x and manual configs allowed
Eth8/2    Yes Yes    cts dot1x and manual configs allowed
Eth8/18   Yes Yes    cts dot1x and manual configs allowed
Eth8/34   Yes Yes    cts dot1x and manual configs allowed
Eth6/3    Yes Yes    cts dot1x and manual configs allowed
Eth8/3    Yes Yes    cts dot1x and manual configs allowed
Eth8/19   Yes Yes    cts dot1x and manual configs allowed
Eth8/35   Yes Yes    cts dot1x and manual configs allowed
Eth6/4    Yes Yes    cts dot1x and manual configs allowed
Eth8/4    Yes Yes    cts dot1x and manual configs allowed
```

```
Eth8/20   Yes Yes    cts dot1x and manual configs allowed
Eth8/36   Yes Yes    cts dot1x and manual configs allowed
Eth6/5    Yes Yes    cts dot1x and manual configs allowed
Eth8/5    Yes Yes    cts dot1x and manual configs allowed
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts	Displays the global Cisco TrustSec configuration.

show cts credentials

To display the Cisco TrustSec device credentials configuration, use the **show cts credentials** command.

show cts credentials

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec credentials configuration:

```
switch# show cts credentials
CTS password is defined in keystore, device-id = Device1
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts environment-data

To display the global Cisco TrustSec environment data, use the **show cts environment-data** command.

show cts environment-data

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

The Cisco NX-OS device downloads the Cisco TrustSec environment data from the ACS after you have configured the Cisco TrustSec credentials for the device and configured authentication, authorization, and accounting (AAA).

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec environment data:

```
switch# show cts environment-data
CTS Environment Data
==============================
  Current State           : CTS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
  Last Status             : CTS_ENV_SUCCESS
  Local Device SGT        : 0x0002
  Transport Type          : CTS_ENV_TRANSPORT_DIRECT
  Data loaded from cache  : FALSE
  Env Data Lifetime       : 300 seconds after last update
  Last Update Time        : Sat Jan  5 16:29:52 2008
  Server List             : ACSServerList1
     AID:74656d706f72617279 IP:10.64.65.95 Port:1812
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts interface

To enable SGT propagation on Layer 2 (L2) Cisco TrustSec interfaces, use the **propagate-sgt** command. To disable SGT propagation, use the **no** form of this command.

propagate-sgt [**l2-control**]

no propagate-sgt [**l2-control**]

Syntax Description

l2-control	Specifies SGT propagation of the L2 control packets.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
8.1(1)	Added the **l2-control** keyword.
6.2(10)	Support was added for F3 Series modules.
4.0(3)	This command was introduced.

Usage Guidelines

You can disable the SGT propagation feature on an interface if the peer device connected to the interface can not handle Cisco TrustSec packets tagged with an SGT.

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown**/**no shutdown** command sequence for the configuration to take effect.

Use the **no propagate-sgt l2-control** command to enable SGT tagging exemption for L2 control packets. This exemption ensures that the L2 control protocols are transmitted without any SGT tags from the Cisco TrustSec enabled-ports. The **no propagate-sgt l2-control** command is supported only on the Cisco M3 Series module ports without Cisco TrustSec MACSec.

You can also enable or disable SGT tagging of the L2 control packets under a port profile and a port channel.

This command requires the Advanced Services license.

Examples

This example shows how to disable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to enable SGT propagation:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to enable SGT tagging exemption for the L2 control protocols.

```
switch# configure terminal
switch(config)# interface ethernet 2/27
switch(config-if)# cts manual
switch(config-if-cts-manual)# no propagate-sgt l2-control
```

This example displays the error message when you enable SGT tagging exemption for the L2 protocols on non-supported modules:

```
switch# configure terminal
switch(config)# interface ethernet 7/2
switch(config-if)# cts manual
switch(config-if-cts-manual)# no propagate-sgt l2-control
ERROR: 'no propagate-sgt l2-control' is not allowed on any port of this line card type.
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec 802.1X configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

show cts l3 interface

To display the Layer 3 Cisco TrustSec configuration on the interfaces, use the **show cts l3 interface** command.

show cts l3 interface

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Layer 3 Cisco TrustSec configuration for the interfaces:

```
switch# show cts l3 interface
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts l3 mapping

To display the Layer 3 Cisco TrustSec mapping configuration for the device, use the **show cts l3 mapping** command.

show cts l3 mapping

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Layer 3 Cisco TrustSec mapping for the device:

```
switch# show cts l3 mapping
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts pacs

To display the Cisco TrustSec protect access credentials (PACs) provisioned by EAP-FAST, use the **show cts pacs** command.

show cts pacs

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec global configuration:

```
switch# show cts pacs
PAC Info :
==============================
  PAC Type            : unknown
  AID                 : 74656d706f72617279
  I-ID                : india1
  AID Info            : ACS Info
  Credential Lifetime : Thu Apr  3 00:36:04 2008
  PAC Opaque          : 0002008300020004000974656d706f7261727900060070000101001d
6321a2a55fa81e05cd705c714bea116907503aab89490b07fcbb2bd455b8d873f21b5b6b403eb1d8
125897d93b94669745cfe1abb0baf01a00b77aacf0bda9fbaf7dcd54528b782d8206a7751afdde42
1ff4a3db6a349c652fea81809fba4f30b1fffb7bfffaf9a6608
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts propagate-status

To display interfaces configured with SGT tagging exemption for L2 control protocols, use the **show cts propagate-status** command.

show cts propagate-status [**interface** {**ethernet***slot/port*| **port-channel** *channel-number*}]

Syntax Description

interface	(Optional) Specifies that the output is limited for a particular interface.
ethernet*slot/port*	(Optional) Specifies that the output is limited to bindings for the Ethernet interface given.
port-channel *channel-number*	(Optional) Specifies that the output is limited to the specified port-channel interface. Valid port-channel numbers are from 1 to 4096.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
8.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

The following example displays all interfaces configured with SGT tagging exemption for L2 control protocols.

```
switch(config)# show cts propagate-status
Interface: Ethernet2/13
Propagate Exemption:
        Protocols: CDP, LLDP, LACP, EAPoL, BPDUs

Interface: Ethernet2/27
Propagate Exemption:
        Protocols: CDP, LLDP, LACP, EAPoL, BPDUs
```

Related Commands

Command	Description
propagate-sgt	Enable SGT propagation on Layer 2 Cisco TrustSec interfaces.
feature cts	Enables the Cisco TrustSec feature.

show cts role-based access-list

To display the global Cisco TrustSec security group access control list (SGACL) configuration, use the **show cts role-based access-list** command.

show cts role-based access-list [*list-name*]

Syntax Description

list-name	(Optional) SGACL name.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.2(1)	Added list name argument.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SGACL configuration:

```
switch# show cts role-based access-list
rbacl:test-3
        deny ip
rbacl:test-1
        deny ip
        deny icmp
        deny tcp src eq 1000 dest eq 2000
        deny udp src range 1000 2000
rbacl:test-2
        permit icmp
        permit igmp
        permit tcp src lt 2000
        permit udp dest gt 4000
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based counters

To display the configuration status of role-based access control list (RBACL) statistics and list the statistics for all RBACL policies, use the **show cts role-based counters** command.

show cts role-based counters [**sgt** {*sgt-value*| **any**| **unknown**}] [**dgt** {*dgt-value*| **any**| **unknown**}]

Syntax Description

sgt	Specifies the source security group tag (SGT).
sgt-value	Source SGT value. The range is from 0 to 65519.
any	Specifies any SGT or DGT.
unknown	Specifies an unknown SGT or DGT.
dgt	Specifies the destination security group tag (DGT).
dgt-value	Destination SGT value. The range is from 0 to 65519.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
8.0(1)	The command output was updated.
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the configuration status of RBACL statistics and the total number of packets that match RBACL policies for a specific SGT and DGT:

```
switch(config)# show cts role-based counters
RBACL policy counters enabled
Counters last cleared: 08/22/2016 at 09:16:07 AM
sgt:unknown dgt:unknown [0]
rbacl:deny_ip(monitored)
deny ip [0]
```

```
sgt:unknown dgt:2000(2000) [0]
rbacl:Deny IP(monitored)
deny ip [0]
sgt:10(10) dgt:20(20) [0]
rbacl:rb1(monitored)
deny udp [0]
permit tcp [0]
deny ip [0]
rbacl:dummy_test (monitored)
permit icmp [0]
permit tcp [0]
permit ip log [0]
sgt:any dgt:any [0]
rbacl:Permit IP(monitored)
permit ip [0]
```

Related Commands

Command	Description
clear cts role-based counters	Clears the RBACL statistics so that all counters are reset to 0.
cts role-based counters enable	Enables the RBACL statistics.

show cts role-based disabled-interface

To display interfaces where Cisco TrustSec security group access control list (SGACL) enforcement policy is disabled, use the **show cts role-based disabled-interface** command.

show cts role-based disabled-interface

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode.

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to verify that SGACL policy enforcement is disabled on interfaces.

```
switch# show cts role-based disabled-interface
Ethernet4/5
Ethernet4/17
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based enable

To display the Cisco TrustSec security group access control list (SGACL) enable status for VLANs and Virtual Routing and Forwarding instances (VRFs), use the **show cts role-based enable** command.

show cts role-based enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SGACL enforcement status:

```
switch# show cts role-based enable
vlan:1
vrf:1
vrf:3
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based policy

To display the global Cisco TrustSec security group access control list (SGACL) policies, use the **show cts role-based policy** command.

show cts role-based policy [sgt{*sgt-value*| **any**| **unknown**}| **dgt**{*dgt-value*| **any**| **unknown**}| **configured**| **downloaded**| **monitored]**

Syntax Description

sgt	Specifies the source security group tag (SGT).
sgt-value	Source SGT value. The range is from 0 to 65535.
any	Specifies any SGT or DGT.
unknown	Specifies an unknown SGT or DGT.
dgt	Specifies the destination security group tag (DGT).
dgt-value	Destination SGT value. The range is from 0 to 65535.
configured	Displays the SGACLs configured by using CLI.
downloaded	Displays the SGACLs downloaded from ISE.
monitored	Displays the monitored SGACLs.

Command Default

None

Command Modes

Any configuration mode.

Command History

Release	Modification
8.0(1)	The **sgt**, **dgt**, **configured**, **downloaded**, and **monitored** keywords were added. Additionally, the command output was updated.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SGACL policies:

```
switch# show cts role-based policy
sgt:unknown
dgt:unknown rbacl:deny_ip(Downloaded,Monitored)
deny ip
sgt:101(101)
dgt:102(102) rbacl:rb2(Configured)
deny eigrp
sgt:101(101)
dgt:102(102) rbacl:ise_rbacl_1_ace(Downloaded)
deny gre
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show cts role-based sgt vlan

To display the Cisco TrustSec Security Group Tag (SGT) mapping configuration for a specific VLAN, use the **show cts role-based sgt vlan** command.

show cts role-based sgt vlan {**all**| *vlan-id*}

Syntax Description

all	Displays the configured SGT for all VLANs.
vlan-id	Configured SGT for the specific VLAN. The range is from 1 to 4094.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec SGT mapping configuration for all VLANs:

```
switch# show cts role-based sgt vlan all
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
show cts role-based sgt-map	Displays the global Cisco TrustSec SGT mapping configuration.
cts role-based sgt	Configures mapping of Cisco TrustSec SGTs to an SGACL.

show cts role-based sgt-map

To display the global Cisco TrustSec Security Group Tag (SGT) mapping configuration, use the **show cts role-based sgt-map** command.

show cts role-based sgt-map [**summary**| **sxp peer** *peer-ipv4-addr*| **vlan** *vlan-id*| **vrf** *vrf-name*]

Syntax Description

summary	(Optional) Displays a summary of the SGT mappings.
sxp peer *peer-ipv4-addr*	(Optional) Displays the SGT map configuration for a specific SGT Exchange Protocol (SXP) peer.
vlan *vlan-id*	(Optional) Displays the SGT map configuration for a specific VLAN.
vrf *vrf-name*	(Optional) Displays the SGT map configuration for a specific virtual routing and forwarding (VRF).

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
6.2(2)	The **summary, sxp peer** *peer-ipv4-addr*, **vlan** *vlan-id*, and **vrf** *vrf-name* keywords and arguments were added.
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec SGT mapping configuration:

```
switch# show cts role-based sgt-map
IP ADDRESS              SGT             VRF/VLAN        SGT CONFIGURATION
5.5.5.5                 5               vlan:10         CLI Configured
5.5.5.6                 6               vlan:10         CLI Configured
5.5.5.7                 7               vlan:10         CLI Configured
5.5.5.8                 8               vlan:10         CLI Configured
10.10.10.10             10              vrf:3           CLI Configured
```

```
10.10.10.20            20              vrf:3           CLI Configured
10.10.10.30            30              vrf:3           CLI Configured
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
cts role-based sgt-map	Manually configures the Cisco TrustSec SGT mapping to IP addresses.

show cts sap pmk

To display the Cisco TrustSec Security Association Protocol (SAP) pairwise master key (PMK) configuration, use the **show cts sap pmk** command.

show cts sap pmk {**all**| **interface ethernet** *slot/port*}

Syntax Description

all	Displays the hexadecimal value of the configured PMK for all interfaces.
interface ethernet *slot/port*	Displays the hexadecimal value of the configured PMK for the specific Ethernet interface.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command does not require a license.

Examples

This example shows how to display the Cisco TrustSec SAP PMK configuration:

```
switch# show cts sap pmk interface ethernet 2/2
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.
sap pmk	Configures the Cisco TrustSec SAP PMK.

show cts sxp

To display Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) connection or source IP-to-SGT mapping information, use the **show cts sxp** command in user EXEC or privileged EXEC mode.

show cts sxp {**connections** | **sgt-map**} [**detail** | **vrf** *instance-name*]

Syntax Description

connections	Displays Cisco TrustSec SXP connections information.
sgt-map	Displays the IP-to-SGT mappings received through SXP.
detail	(Optional) Displays detailed SXP information.
vrf *instance-name*	(Optional) Displays the SXP information for the specified Virtual Routing and Forwarding (VRF) instance name.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	The keywords connections, sgt-map, detail, and vrf were introduced.
7.3(0)D1(1)	The output was modified to include details about the SXPv3 version and network map expansion limit.
4.0(1)	This command was introduced.

Examples

The following example displays the CTS-SXP connections:

```
switch# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
```

```
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections for a bi-directional connection when the device is both the speaker and listener:

```
switch# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
----------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

The following example displays output from a CTS-SXP listener with a torn down connection to the SXP speaker. Source IP-to-SGT mappings are held for 120 seconds, the default value of the Delete Hold Down timer.

```
switch# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : Delete_Hold_Down
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
```

```
Set up          : Peer
Conn status     : On
Connection inst# : 1
TCP conn fd     : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

Related Commands

Command	Description
cts sxp connection peer	Enters the Cisco TrustSec SXP peer IP address and specifies if a password is used for the peer connection
cts sxp default password	Configures the Cisco TrustSec SXP default password.
cts sxp default source-ip	Configures the Cisco TrustSec SXP source IPv4 address.
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the Cisco TrustSec SXP reconciliation period.
cts sxp retry	Changes the Cisco TrustSec SXP retry period timer.

show cts sxp connection

To display the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SXP) connections information, use the **show cts sxp connection** command.

show cts sxp connection

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SXP) connections information:

```
switch# show cts sxp connection
PEER_IP_ADDR  VRF        PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE    VERSION
30.1.1.3      default    listener        speaker         connected           3
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show data-corruption

To display data inconsistency errors, use the **show data-corruption** command.

show data-corruption

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display the data inconsistency errors:

```
switch# show data-corruption
DATACORRUPTION-DATAINCONSISTENCY: -Traceback= vmtracker libhmm_dll.so+0x1b4d0 libhmm.so+0x2cf0
 libhmm_dll.so +0x1ba0a libhmm_dll.so+0x1c9e7 libhmm.so+0x2f49 +0x209d0
libvmtracker.so+0x4d586 libvmtracker.so+0x9b0c1 libvmtracker.so+0x43154 libvmtracker.so+0x42c
 happened 20 times since Mon Feb 15 09:05:20 2016
DATACORRUPTION-DATAINCONSISTENCY: -Traceback= hmm +0x40faf +0xbf870 +0xc0b4c +0x40292
+0xa37fa +0xa9f29 +0xc05aa +0xc060e +0xc0765 +0x42c35 +0x2c339 librsw.so+0xacc33
libpthread.so.0+0x6b75 libc.so.6+0xee02e happened 1 time since Fri Feb 12 00:01:16 2016
```

show dot1x

To display the 802.1X feature status, use the **show dot1x** command.

show dot1x

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the 802.1X feature status:

```
switch# show dot1x
           Sysauthcontrol Enabled
   Dot1x Protocol Version 2
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

show dot1x all

To display all 802.1X feature status and configuration information, use the **show dot1x all** command.

show dot1x all [**details**| **statistics**| **summary**]

Syntax Description

details	(Optional) Displays detailed information about the 802.1X configuration.
statistics	(Optional) Displays 802.1X statistics.
summary	(Optional) Displays a summary of 802.1X information.

Command Default

Displays global and interface 802.1X configuration

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display all 802.1X feature status and configuration information:

```
switch# show dot1x all
           Sysauthcontrol Enabled
   Dot1x Protocol Version 2
Dot1x Info for Ethernet2/1
-----------------------------------
                      PAE = AUTHENTICATOR
              PortControl = FORCE_AUTH
                 HostMode = SINGLE HOST
         ReAuthentication = Disabled
              QuietPeriod = 60
            ServerTimeout = 30
              SuppTimeout = 30
             ReAuthPeriod = 3600 (Locally configured)
                ReAuthMax = 2
                   MaxReq = 2
                 TxPeriod = 30
          RateLimitPeriod = 0
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

show dot1x interface ethernet

To display the 802.1X feature status and configuration information for an Ethernet interface, use the **show dot1x interface ethernet** command.

show dot1x interface ethernet *slot/port* [**details**| **statistics**| **summary**]

Syntax Description

slot/port/	Slot and port identifiers for the interface.
details	(Optional) Displays detailed 802.1X information for the interface.
statistics	(Optional) Displays 802.1X statistics for the interface.
summary	(Optional) Displays a summary of the 802.1X information for the interface.

Command Default

Displays the interface 802.1X configuration

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the 802.1X feature status and configuration information for an Ethernet interface:

```
switch# show dot1x interface ethernet 2/1
Dot1x Info for Ethernet2/1
-----------------------------------
                      PAE = AUTHENTICATOR
              PortControl = FORCE_AUTH
                 HostMode = SINGLE_HOST
         ReAuthentication = Disabled
              QuietPeriod = 60
            ServerTimeout = 30
              SuppTimeout = 30
             ReAuthPeriod = 3600 (Locally configured)
                ReAuthMax = 2
              MaxReq = 2
            TxPeriod = 30
     RateLimitPeriod = 0
```

Related Commands

Command	Description
feature dot1x	Enables the 802.1X feature.

show encryption service stat

To display the status of the encryption service, use the **show encryption service stat** command.

show encryption service stat

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the status of the encryption service:

```
switch# show encryption service stat
Encryption service is enabled
Master Encryption Key is configured.
Type-6 encryption is being used
switch#
```

Related Commands

Command	Description
show key chain	Displays the configuration for a specific keychain.

show eou

To display Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) status and configuration information, use the **show eou** command.

show eou [**all**| **authentication** {**clientless**| **eap**| **static**}| **interface ethernet***slot/port*| **ip-address** *ipv4-address*| **mac-address** *mac-address*| **posturetoken** *[name]*]

Syntax Description

all	(Optional) Displays all EAPoUDP sessions.
authentication	(Optional) Displays EAPoUDP sessions for specific authentication types.
clientless	Specifies sessions authenticated using clientless posture validation.
eap	Specifies sessions authenticated using EAPoUDP.
static	Specifies sessions statically authenticated using statically configured exception lists.
interface ethernet *slot/port*	(Optional) Displays the EAPoUDP sessions for a specific interface.
ip-address*ipv4-address*	(Optional) Displays the EAPoUDP sessions for a specific IPv4 address.
mac-address*mac-address*	(Optional) Displays the EAPoUDP sessions for a specific MAC address.
posturetoken *[name]*	(Optional) Displays the EAPoUDP sessions for posture tokens.
name	(Optional) Token name.

Command Default

Displays the global EAPoUDP configuration

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature eou** command before using this command.

This command does not require a license.

Examples

This example shows how to display all 802.1X feature status and configuration information:

```
switch# show eou all
```

This example shows how to display 802.1X clientless authentication information:

```
switch# show eou authentication clientless
```

This example shows how to display 802.1X EAP authentication information:

```
switch# show eou authentication eap
```

This example shows how to display 802.1X static authentication information:

```
switch# show eou interface ethernet 2/1
```

This example shows how to display 802.1X information for an Ethernet interface:

```
switch# show eou ip-address 10.10.10.1
```

This example shows how to display 802.1X information for a MAC address:

```
switch# show eou mac-address 0019.076c.dac4
```

This example shows how to display 802.1X information for a MAC address:

```
switch# show eou posturetoken healthy
```

Related Commands

Command	Description
feature eou	Enables the 802.1X feature.

show fips status

To display the status of Federal Information Processing Standards (FIPS) mode, use the **show fips** *status* command.

show fips status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the status of FIPS mode:

```
switch# show fips status
FIPS mode is disabled
```

Related Commands

Command	Description
fips mode enable	Enables FIPS mode.

show hardware access-list feature-combo

To display the bank mapping matrix, use the **show hardware access-list feature- combo** command.

show hardware access-list {**input**| **output**} {**interface**| **vlan**} **feature-combo** *features*

Syntax Description

input	Displays input/ingress policies.
output	Displays output/egress policies..
interface	Specifies interface.
vlan	Specifies VLAN.
feature-combo	Specifies the feature combination.
features	Specifies the features.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(10)	This command was introduced.

Usage Guidelines

This command does not require a license.

The following are the features you can enter:

- arp—Address Resolution Protocol
- bfd—Bidirectional Forwarding Detection
- cbts—Class-Based Tunnel Selection
- cts_impl_tunnel—CTS Implicit Tunnel
- dhcp—Dynamic Host Configuration Protocol
- erspan_dst—Encapsulated Remote Switched Port Analyzer (destination)
- erspan_src—Encapsulated Remote Switched Port Analyzer (source)
- lisp—Locator/ID Separation Protocol

- lisp_inst—LISP Multitenant Policy
- netflow—NetFlow
- netflow_svi—NetFlow on SVI
- netflow_sampler—NetFlow Sampler
- netflow_sampler_svi—NetFlow Sampler on SVI
- otv—Overlay Transport Virtualization
- pacl—Port ACL
- pbr—Policy-Based Routing without statistics
- pbr_stats—Policy-Based Routing with statistics
- qos—Quality of Service
- racl—Router ACL without statistics
- racl_stats—Router ACL with statistics
- rbacl—Role-based ACL
- tunnel-decap—Tunnel Decap
- vacl—VLAN ACL without statistics
- vacl_stats—VLAN ACL with statistics
- wccp—Web Cache Communication Protocol

If the feature is not supported, the switch returns the following message:

```
This feature combination is not supported !
```

Examples

This example shows how to display a feature combination check on the ingress policy on a Layer 3 interface with the following features—racl with no stats, pbr with stats, wccp, qos and netflow:

```
switch# show hardware access-list input interface feature-combo racl pbr_stats wccp qos
netflow
______________________________________________________________________________
Feature                     Rslt Type     T0B0      T0B1      T1B0      T1B1
______________________________________________________________________________
RACL Interface                  Acl         X
Netflow                         Acl         X
QoS Interface                   Qos                             X
WCCP Interface                  Acl         X
PBR Interface Stats             Acl                   X
```

This example shows how to display a feature combination check on the ingress policy on a VLAN/SVI with the following features—vacl with stats, racl on svi, pbr on svi, dhcp snoop on vlan and wccp:

```
switch# show hardware access-list input vlan feature-combo vacl_stat racl pbr dhcp wccp
______________________________________________________________________________
Feature                     Rslt Type     T0B0      T0B1      T1B0      T1B1
______________________________________________________________________________
RACL                            Acl                                       X
PBR                             Acl                                       X
DHCP                            Acl                             X
SPM WCCP                        Acl                                       X
VACL Stats                      Acl                             X
```

This example shows how to display a f eature combination check on the ingress policy on a Layer 2 interface with the following features —pacl and l2 qos:

```
switch# show hardware access-list input vlan feature-combo pacl
------------------------------------------------------------------------------
Feature                     Rslt Type      T0B0      T0B1      T1B0      T1B1
------------------------------------------------------------------------------
PACL                           Acl          X
QoS                            Qos                    X
```

Related Commands

Command	Description
hardware access-list resource feature bank-mapping	Configures the device to allow ACL TCAM bank mappings.

show hardware rate-limiter

To display the hardware rate limit configuration and statistics, use the **show hardware rate-limiter** command.

show hardware rate-limiter {**access-list-log** [**module** *module*]| **copy** [**module** *module*]| **f1** {**rl-1** [**module** *module*]| **rl-2** [**module** *module*]| **rl-3** [**module** *module*]| **rl-4** [**module** *module*]| **rl-5** [**module** *module*]}| **layer-2** {**l2pt** [**module** *module*]| **mcast-snooping** [**module** *module*]| **port-security** [**module** *module*]| **storm-control** [**module** *module*]| **vpc-low** [**module** *module*]}| **layer-3** {**control** [**module** *module*]| **glean** [**module** *module*]| **glean-fast** [**module** *module*] **mtu** [**module** *module*]| **multicast** {**directly-connect** [**module** *module*]| **local-groups** [**module** *module*]| **rpf-leak** [**module** *module*]}| **ttl** [**module** *module*]}| **module** *module*| **receive** [**module** *module*]}

Syntax Description

access-list-log	Specifies rate-limit statistics for access-list log packets.
module*module*	Specifies a module number. The range is from 1 to 18.
copy	Specifies rate-limit statistics for copy packets.
f1	Specifies the control packets from the F1 modules to the supervisor.
rl-1	Specifies the F1 rate-limiter 1.
rl-2	Specifies the F1 rate-limiter 2.
rl-3	Specifies the F1 rate-limiter 3.
rl-4	Specifies the F1 rate-limiter 4.
rl-5	Specifies the F1 rate-limiter 5.
layer-2	(Optional) Displays Layer 2 packet rate limits.
l2pt	Specifies rate-limit statistics for Layer 2 Tunnel Protocol (L2TP) packets.
mcast-snooping	Specifies rate-limit statistics for Layer 2 multicast-snooping packets.
port-security	Specifies rate-limit statistics for Layer 2 port-security packets.
storm-control	Specifies rate-limit statistics for Layer 2 storm-control packets.

vpc-low	Specifies rate-limit statistics for Layer 2 control packets over the virtual port channel (vPC) low queue.
layer-3	(Optional) Displays Layer 3 packet rate limits.
control	Specifies rate-limit statistics for Layer 3 control packets.
glean	Specifies rate-limit statistics for Layer 3 glean packets.
glean-fast	Specifies rate-limit statistics for Layer 3 glean fast-path packets.
mtu	Specifies rate-limit statistics for Layer 3 maximum transmission unit (MTU) packets.
multicast	Specifies Layer 3 multicast rate limits.
directly-connected	Specifies rate-limit statistics for Layer 3 directly connected multicast packets.
local-groups	Specifies rate-limit statistics for Layer 3 local group multicast packets.
rpf-leak	Specifies rate-limit statistics for Layer 3 reverse path forwarding (RPF) leak multicast packets.
ttl	Specifies rate-limit statistics for Layer 3 time-to-live (TTL) packets.
receive	(Optional) Displays rate-limit statistics for receive packets.

Command Default

Displays all rate-limit statistics.

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	Added the glean-fast keyword.
5.1(1)	Added the f1, rl-1, rl-2, rl-3, rl-4, rl-5, and module keywords.
5.0(2)	Added the **l2pt** keyword.

Release	Modification
4.0(3)	Added the **port-security** keyword.
4.0(1)	This command was introduced.

Usage Guidelines

You can use the command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display all the hardware rate-limit configuration and statistics:

```
switch# show hardware rate-limiter
Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters
Rate Limiter Class                       Parameters
------------------------------------------------------------
layer-3 mtu                              Config    : 500
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-3 ttl                              Config    : 500
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-3 control                          Config    : 10000
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-3 glean                            Config    : 100
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-3 multicast directly-connected     Config    : 3000
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-3 multicast local-groups           Config    : 3000
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-3 multicast rpf-leak               Config    : 500
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-2 storm-control                    Config    : Disabled
access-list-log                          Config    : 100
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
copy                                     Config    : 30000
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
receive                                  Config    : 30000
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-2 port-security                    Config    : Disabled
layer-2 mcast-snooping                   Config    : 10000
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-2 vpc-low                          Config    : 4000
```

```
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
layer-2 l2pt                             Config    : 500
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
```

This example shows how to display the rate-limit configuration and statistics for access-list log packets:

```
switch# show hardware rate-limiter access-list-log
Units for Config: packets per second
Allowed, Dropped & Total: aggregated since last clear counters
Rate Limiter Class                       Parameters
------------------------------------------------------------
access-list-log                          Config    : 100
                                         Allowed   : 0
                                         Dropped   : 0
                                         Total     : 0
```

Related Commands

Command	Description
clear hardware rate-limiter	Clears rate-limit statistics.
hardware rate-limiter	Configures rate limits.

show identity policy

To display the identity policies, use the **show identity policy** command.

show identity policy [*policy-name*]

Syntax Description

policy-name	(Optional) Name of a policy. The name is case sensitive.

Command Default

Displays information for all identity policies.

Command Modes

Any command mode

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 display information for all of the identity policies:

```
switch# show identity policy
```

This example shows how to display information for a specific identity policy:

```
switch# show identity policy AdminPolicy
```

Related Commands

Command	Description
identity policy	Configures identity policies.

show identity profile

To display the identity profiles, use the **show identity profile** command.

show identity profile [eapoudp]

Syntax Description

eapoudp	(Optional) Displays the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) identity profile.

Command Default

Displays information for all identity profiles.

Command Modes

Any command mode

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 display the identity profiles:

```
switch# show identity profile
```

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

```
switch# show identity profile eapoudp
```

Related Commands

Command	Description
identity profile eapoudp	Configures EAPoUDP identity profiles.

show ip access-lists

To display all IPv4 access control lists (ACLs) or a specific IPv4 ACL, use the **show ip access-lists** command.

show ip access-lists [*access-list-name*] [**expanded**| **summary**]

Syntax Description

access-list-name	(Optional) Name of an IPv4 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
expanded	(Optional) Specifies that the contents of IPv4 address groups or port groups show rather than the names of object groups only.
summary	(Optional) Specifies that the command displays information about the ACL rather than the ACL configuration. For more information, see the “Usage Guidelines” section.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names. Support was added for the **fragments** command.
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all IPv4 ACLs, unless you use the *access-list-name* argument to specify an ACL.

If you do not specify an ACL name, the device lists ACLs alphabetically by the ACL names.

IPv4 address object groups and IP port object groups show only by name, unless you use the **expanded** keyword.

The **expanded** keyword allows you to display the details of object groups used in an ACL rather than only the name of the object groups. For more information about object groups, see the **object-group ip address** and **object-group ip port** commands.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics are configured for the ACL.
- Whether the **fragments** command is configured for the ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries that the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show ip access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

If an IP ACL includes the **fragments** command, it appears before the explicit permit and deny rules, but the device applies the **fragments** command to noninitial fragments only if they do not match all other explicit rules in the ACL.

This command does not require a license.

Examples

This example shows how to use the **show ip access-lists** command to display all IPv4 ACLs on a device that has a single IPv4 ACL:

```
switch# show ip access-lists
IP access list ipv4-open-filter
        10 permit ip any any
```

This example shows how to use the **show ip access-lists** command to display an IPv4 ACL named ipv4-RandD-outbound-web, including per-entry statistics for the entries except for the MainLab object group:

```
switch# show ip access-lists ipv4-RandD-outbound-web
IP access list ipv4-RandD-outbound-web
        statistics per-entry
        fragments deny-all
        1000 permit ahp any any [match=732]
        1005 permit tcp addrgroup MainLab any eq telnet
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show ip access-lists** command to display an IPv4 ACL named ipv4-RandD-outbound-web. The **expanded** keyword causes the contents of the object group from the previous example to appear, including the per-entry statistics:

```
switch# show ip access-lists ipv4-RandD-outbound-web expanded
IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp 10.52.34.4/32 any eq telnet [match=5032]
        1005 permit tcp 10.52.34.27/32 any eq telnet [match=433]
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show ip access-lists** command with the **summary** keyword to display information about an IPv4 ACL named ipv4-RandD-outbound-web, such as which interfaces the ACL is applied to and active on:

```
switch# show ip access-lists ipv4-RandD-outbound-web summary
IPV4 ACL ipv4-RandD-outbound-web
        Statistics enabled
```

```
Total ACEs Configured: 4
Configured on interfaces:
        Ethernet2/4 - ingress (Router ACL)
Active on interfaces:
        Ethernet2/4 - ingress (Router ACL)
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ip access-list	Configures an IPv4 ACL.
show access-lists	Displays all ACLs or a specific ACL.
show ipv6 access-lists	Displays all IPv6 ACLs or a specific IPv6 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
statistics per-entry	Starts recording statistics for packets permitted or denied by each entry in an ACL.

show ip access-lists capture session

To display the ACL capture session configuration, use the **show ip access-lists capture session** command.

show ip access-lists capture session *session*

Syntax Description

session	Session ID. The range is from 0 to 4294967295.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the ACL capture session configuration:

```
switch# show ip access-lists capture session 5
switch#
```

Related Commands

Command	Description
monitor session *session* **type acl-capture**	Configures an ACL capture session.
destination interface	Configures a destination for ACL capture packets.

show ip arp inspection

To display the Dynamic ARP Inspection (DAI) configuration status, use the **show ip arp inspection** command.

show ip arp inspection

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the status of the DAI configuration:

```
switch# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled
Vlan : 1
-----------
Configuration    : Enabled
Operation State  : Active
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

Related Commands

Command	Description
ip arp inspection vlan	Enables DAI for a specified list of VLANs.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.

Command	Description
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection statistics	Displays the DAI statistics.
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.

show ip arp inspection interface

To display the trust state and the ARP packet rate for the specified interface, use the **show ip arp inspection interface** command.

Syntax Description

show ip arp inspection interfaceethernet *slot/port*| **port-channel** *channel-number*

ethernet *slot /port*	(Optional) Specifies that the output is for an Ethernet interface.
port-channel *channel-number*	(Optional) Specifies that the output is for a port-channel interface. Valid port-channel numbers are from 1 to 4096.

Command Default

None

Command Modes

Any command mode

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 display the trust state and the ARP packet rate for a trusted interface:

```
switch# show ip arp inspection interface ethernet 2/1

 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet2/46        Trusted         15              5
switch#
```

Related Commands

Command	Description
ip arp inspection vlan	Enables Dynamic ARP Inspection (DAI) for a specified list of VLANs.
show ip arp inspection	Displays the DAI configuration status.

Command	Description
show ip arp inspection log	Displays the DAI log configuration.
show ip arp inspection statistics	Displays the DAI statistics.
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.

show ip arp inspection log

To display the Dynamic ARP Inspection (DAI) log configuration, use the **show ip arp inspection log** command.

show ip arp inspection log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the DAI log configuration:

```
switch# show ip arp inspection log

Syslog Buffer Size : 32
Syslog Rate        : 5 entries per 1 seconds
switch#
```

Related Commands

Command	Description
clear ip arp inspection log	Clears the DAI logging buffer.
ip arp inspection log-buffer	Configures the DAI logging buffer size.
show ip arp inspection	Displays the 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.

show ip arp inspection statistics

Use the **show ip arp inspection statistics** command to display the Dynamic ARP Inspection (DAI) statistics. You can specify a VLAN or range of VLANs.

show ip arp inspection statistics [**vlan** *vlan-list*]

Syntax Description

vlan *vlan-list*	(Optional) Specifies the list of VLANs for which to display DAI statistics. Valid VLAN IDs are from 1 to 4096.

Command Default

None

Command Modes

Any command mode

Supported User Roles

network-admin

network-operator

vdc-admin

vdc-operator

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 display the DAI statistics for VLAN 1:

```
switch# show ip arp inspection statistics vlan 1

Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switch#
```

Related Commands

Command	Description
clear ip arp inspection statistics vlan	Clears the DAI statistics for a specified VLAN.
show ip arp inspection	Displays the DAI configuration status.
show ip arp inspection interface	Displays the trust state and the ARP packet rate for a specified interface.
show ip arp inspection log	Displays the DAI log configuration.
show running-config dhcp	Displays DHCP snooping configuration, including DAI configuration.

show ip arp inspection vlan

Use the **show ip arp inspection vlan** command to display Dynamic ARP Inspection (DAI) status for the specified list of VLANs.

show ip arp inspection vlan *vlan-list*

Syntax Description

vlan-list	VLANs with DAI status that this command shows. 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.

Command Default

None

Command Modes

Any command mode

Supported User Roles

network-admin

network-operator

vdc-admin

vdc-operator

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

This example shows how to display DAI status for VLANs 1 and 13:

```
switch# show ip arp inspection vlan 1,13

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled
Vlan : 1
-----------
Configuration    : Enabled
Operation State  : Active
Vlan : 13
-----------
Configuration    : Enabled
Operation State  : Inactive
switch#
```

Related Commands

Command	Description
clear ip arp inspection statistics vlan	Clears the DAI statistics for a specified VLAN.
ip arp inspection vlan	Enables DAI for a specified list of VLANs.
show ip arp inspection	Displays the 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.

show ip device tracking

To display IP device tracking information, use the **show ip device tracking** command.

show ip device tracking all| interface ethernet *slot/port*| **ip-address** *ipv4-address*| **mac-address** *mac-address*

Syntax Description

all	Displays all IP device tracking information.
interface ethernet *slot/port*	Displays IP tracking device information for an interface.
ip-address*ipv4-address*	Displays IP tracking device information for an IPv4 address in the A.B.C.D format.
mac-address*mac-address*	Displays IP tracking information for a MAC address in the XXXX.XXXX.XXXX format.

Command Default

None

Command Modes

Any command mode

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 display all IP device tracking information:

```
switch# show ip device tracking all
```

This example shows how to display the IP device tracking information for an interface:

```
switch# show ip device tracking ethernet 1/2
```

This example shows how to display the IP device tracking information for an IP address:

```
switch# show ip device tracking ip-address 10.10.1.1
```

This example shows how to display the IP device tracking information for a MAC address:

```
switch# show ip device tracking mac-address 0018.bad8.3fbd
```

Related Commands

Command	Description
ip device tracking	Configures IP device tracking.

show ip dhcp relay

To display DHCP snooping relay status, including DHCP server address configuration details, use the **show ip dhcp relay** command.

show ip dhcp relay

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.
7.2(0)D1(1)	This command was modified. An example for a helper address configuration on a bridge domain interface (BDI) was added.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the DHCP relay status and configured DHCP server addresses:

```
switch# show ip dhcp relay
DHCP relay service is enabled
Insertion of option 82 is enabled
Insertion of VPN suboptions is enabled
Helper addresses are configured on the following interfaces:
 Interface        Relay Address     VRF Name
 -------------    -------------     --------
 Ethernet1/4       10.10.10.1       red
```

This example shows how to display the DHCP relay status and configured DHCP server addresses. In this example, the helper address is configured on a bridge domain interface.

```
switch# show ip dhcp relay
DHCP relay service is enabled
Insertion of option 82 is enabled
Insertion of VPN suboptions is enabled
Global smart-relay is disabled
Relay Trusted Port is Globally disabled
Relay Trusted functionality is disabled
Smart-relay is enabled on the following interfaces:
-----------------------------------------------------
Subnet-broadcast is enabled on the following interfaces:
------------------------------------------------------
Helper addresses are configured on the following interfaces:
Interface        Relay Address     VRF Name
```

```
 -------------    -------------     --------
Bdi14  192.0.2.120      management
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp relay	Enables the DHCP relay agent.
show ip dhcp relay address	Shows DHCP server addresses configured on the device.

show ip dhcp relay address

To display DHCP server addresses configured on the device, use the **show ip dhcp relay address** command.

show ip dhcp relay address [**interface** {**ethernet** *list*| **port-channel** *list*}]

show ip dhcp relay address [**interface** *interface-list*]

Syntax Description

interface	(Optional) Restricts the output to a DHCP addresses configured on range or set of Ethernet or port-channel interfaces and subinterfaces.
ethernet	(Optional) Restricts the output to a DHCP addresses configured on range or set of Ethernet interfaces and subinterfaces.
list	Single interface, range of interfaces, or comma-separated interfaces and ranges (see the "Examples" section).
port-channel	(Optional) Restricts the output to a DHCP addresses configured on range or set of port-channel interfaces and subinterfaces.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	Support was added for the **interface** keyword and for VRF awareness.
4.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display all the DHCP relay addresses configured on a device:

```
switch# show ip dhcp relay address
 Interface        Relay Address     VRF Name
 -------------    -------------     --------
 Ethernet1/2       10.1.1.1
 Ethernet1/3       10.1.1.1         red
 Ethernet1/4       10.1.1.1         red
 Ethernet1/5       10.1.1.1         red
 Ethernet1/6       10.1.1.1         red
 Ethernet1/7       10.1.1.1         red
 Ethernet1/8       10.1.1.1         red
switch#
```

This example shows how to display the DHCP relay addresses configured Ethernet interfaces 1/2 through 1/4 and Ethernet 1/8:

```
switch(config-if)# show ip dhcp relay address interface ethernet 1/2-4,ethernet 1/8
 Interface        Relay Address     VRF Name
 -------------    -------------     --------
 Ethernet1/2       10.1.1.1
 Ethernet1/3       10.1.1.1         red
 Ethernet1/4       10.1.1.1         red
 Ethernet1/8       10.1.1.1         red
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp relay	Enables the DHCP relay agent.
show ip dhcp relay	Shows DHCP relay status and server addresses configured on the device.

show ip dhcp relay statistics

To display the DHCP relay statistics, use the **show ip dhcp relay statistics** command.

show ip dhcp relay statistics [**interface** *interface*]

Syntax Description

interface*interface*	Displays the DHCP relay address of the interface. The supported interface types are ethernet, port-channel, and VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.
7.2(0)D1(1)	This command was modified. An example for DHCP relay statistics information for a Bridge Domain Interface (BDI) was added.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display DHCP relay statistics for an interface:

```
switch# show ip dhcp relay statistics interface bdi 14
--------------------------------------------------------
Message Type             Rx              Tx           Drops
----------------------------------------------------------------------
Discover                  7               7               0
Offer                     0               0               0
Request(*)                0               0               0
Ack                       0               0               0
Release(*)                0               0               0
Decline                   0               0               0
Inform(*)                 0               0               0
Nack                      0               0               0
----------------------------------------------------------------------
Total                     7               7               0
----------------------------------------------------------------------
DHCP server stats:
----------------------------------------------------------------------------
Server           Vrf                                 Request       Response
----------------------------------------------------------------------------
10.64.66.242     management                                7              0
----------------------------------------------------------------------
```

```
DHCP L3 FWD:
Total Packets Received                           : 0
Total Packets Forwarded                       :    0
Total Packets Dropped                            :         0
Non DHCP:
Total Packets Received                            :         0
Total Packets Forwarded                        :         0
```

Related Commands

Command	Description
ip dhcp relay	Enables the DHCP relay agent.
show ip dhcp relay	Displays the DHCP configuration.

show ip dhcp snooping

To display general status information for DHCP snooping, use the **show ip dhcp snooping** command.

show ip dhcp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Displayed Statistics

- **Packets processed—**The number of packets containing DHCP messages.
- **Packets forwarded—**The number of packets containing DHCP messages forwarded by the relay agent.
- **Total packets dropped—**The total number of packets containing DHCP messages that were dropped. The reasons for dropping the packets are as follows:
  - **Received from untrusted ports—**The number of packets containing DHCP messages, particularly DHCPOFFER packets, received from untrusted ports.
  - **MAC address check failure—**
  - **Option 82 insertion failure—**
  - **O/P Intf unknown—**
  - **Unknown reason—**

Examples

This example shows how to display general status information about DHCP snooping:

```
switch# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
```

```
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust/rate is configured on the following interfaces:
Interface            Trusted         Rate limit (pps)
------------         -------         ----------------
Ethernet2/3          Yes
switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp snooping	Globally enables DHCP snooping on the device.
show ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.
show ip dhcp snooping statistics	Displays DHCP snooping statistics.
show running-config dhcp	Displays DHCP snooping configuration.

show ip dhcp snooping binding

To display IP-to-MAC address bindings for all interfaces or a specific interface, use the **show ip dhcp snooping binding** command. It includes static IP source entries. Static entries appear with the term “static” in the Type column.

show ip dhcp snooping binding [*IP-address*][*MAC-address*] [**interface ethernet** *slot/port*] [**vlan***vlan-id*]

show ip dhcp snooping binding [dynamic]

show ip dhcp snooping binding [static]

Syntax Description

IP-address	(Optional) IPv4 address that the bindings shown must include. Valid entries are in dotted-decimal format.
MAC-address	(Optional) MAC address that the bindings shown must include. Valid entries are in dotted-hexadecimal format.
interface ethernet*slot/port* /	(Optional) Specifies the Ethernet interface that the bindings shown must be associated with.
vlan *vlan-id*	(Optional) Specifies a VLAN ID that the bindings shown must be associated with. Valid VLAN IDs are from 1 to 4096.
dynamic	(Optional) Limits the output to all dynamic IP-MAC address bindings.
static	(Optional) Limits the output to all static IP-MAC address bindings.

Command Default

None

Command Modes

Any command mode

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 display all bindings:

```
switch# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type        VLAN  Interface
-----------------  ---------------  --------  ----------  ----  -------------
0f:00:60:b3:23:33  10.3.2.2         infinite  static      13    Ethernet2/46
0f:00:60:b3:23:35  10.2.2.2         infinite  static      100   Ethernet2/10
switch#
```

Related Commands

Command	Description
clear ip dhcp snooping binding	Clears the DHCP snooping binding database.
feature dhcp	Enables the DHCP snooping feature on the device.
ip dhcp relay	Enables or disables 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 ip dhcp snooping statistics	Displays DHCP snooping statistics.
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

show ip dhcp snooping statistics

To display DHCP snooping statistics, use the **show ip dhcp snooping statistics** command.

show ip dhcp snooping statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Displayed Statistics

- **Packets processed—**The number of packets containing DHCP messages.
- **Packets forwarded—**The number of packets containing DHCP messages forwarded by the relay agent.
- **Total packets dropped—**The total number of packets containing DHCP messages that were dropped. The reasons for dropping the packets are as follows:
    - **Received from untrusted ports—**The number of packets containing DHCP messages, particularly DHCPOFFER packets, received from untrusted ports.
    - **MAC address check failure—**
    - **Option 82 insertion failure—**
    - **O/P Intf unknown—**
    - **Unknown reason—**

Examples

This example shows how to display DHCP snooping statistics:

```
switch# show ip dhcp snooping statistics
Packets processed 0
Packets received through cfsoe 0
Packets forwarded 0
Packets forwarded on cfsoe 0
Total packets dropped 0
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to dhcp relay not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 0
Packets dropped due to max hops exceeded 0
switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
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 ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.
show running-config dhcp	Displays DHCP snooping configuration.

show ip udp relay

To display the configuration details of the UDP relay feature, use the show ip udp relay command.

show ip udp relay [**interface** [**ethernet** *slot/port-number*| **port-channel** *port-channel-number*]| **object-group** *object-group-name*]

Syntax Description

slot/port-number	Specifies the slot and port number.
port-channel-number	Specifies the port channel number.
object-grp-name	Specifies the name of the object group.

Command Default

None

Command Modes

Any command mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the details of the UDP relay feature:

```
switch# show ip udp relay
UDP relay service is enabled
UDP relay on default UDP ports:
Default UDP Ports Status
-------------------------- -------------
Time service                   (port 37 ) enabled
IEN-116 Name Service           (port 42 ) enabled
TACACS service                 (port 49 ) enabled
Domain Naming System           (port 53 ) enabled
Trivial File Transfer Protocol (port 69 ) enabled
NetBIOS Name Server            (port 137) enabled
NetBIOS Datagram Server        (port 138) enabled
UDP relay is enabled on the following non-default UDP ports:
-----------------------------------------------------------------
Object-group and Subnet-broadcast configurations:
Interface Subnet-broadcast Object-group
---------- ---------------- ------------
Vlan700 disabled iSmart
Vlan800 enabled iHello
```

Related Commands

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

show ip verify source

To display the IP-to-MAC address bindings, use the **show ip verify source** command.

show ip verify source [**interface** {**ethernet***slot/port*| **port-channel** *channel-number*}]

Syntax Description

interface	(Optional) Specifies that the output is limited to IP-to-MAC address bindings for a particular interface.
ethernet*slot/port*	(Optional) Specifies that the output is limited to bindings for the Ethernet interface given.
port-channel *channel-number*	(Optional) Specifies that the output is limited to bindings for the port-channel interface given. Valid port-channel numbers are from 1 to 4096.

Command Default

None

Command Modes

Any command mode

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 display the IP-to-MAC address bindings:

```
switch# show ip verify source
switch#
```

Related Commands

Command	Description
ip source binding	Creates a static IP source entry for the specified Ethernet interface.
ip verify source dhcp-snooping-vlan	Enables IP Source Guard on an interface.

Command	Description
show running-config dhcp	Displays DHCP snooping configuration, including IP Source Guard configuration.

show ipv6 access-lists

To display all IPv6 access-control lists (ACLs) or a specific IPv6 ACL, use the **show ipv6 access-lists** command.

show ipv6 access-lists [*access-list-name*] [**expanded**| **summary**]

Syntax Description

access-list-name	(Optional) Name of an IPv6 ACL, which can be up to 64 alphanumeric, case-sensitive characters.
expanded	(Optional) Specifies that the contents of IPv6 address groups or port groups show rather than the names of object groups only.
summary	(Optional) Specifies that the command displays information about the ACL rather than the ACL configuration. For more information, see the “Usage Guidelines” section.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names. Support was added for the **fragments** command.
4.1(2)	This command was introduced.

Usage Guidelines

The device shows all IPv6 ACLs, unless you use the *access-list-name* argument to specify an ACL.

If you do not specify an ACL name, the device lists ACLs alphabetically by the ACL names.

IPv6 address object groups and IP port object groups show only by name, unless you use the **expanded** keyword.

The **expanded** keyword allows you to display the details of object groups used in an ACL rather than only the name of the object groups. For more information about object groups, see the **object-group ipv6 address** and **object-group ip port** commands.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics are configured for the ACL.
- Whether the **fragments** command is configured for the ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries that the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.
- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show ipv6 access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

If an IP ACL includes the **fragments** command, it appears before the explicit permit and deny rules, but the device applies the **fragments** command to noninitial fragments only if they do not match all other explicit rules in the ACL.

This command does not require a license.

Examples

This example shows how to use the **show ipv6 access-lists** command to display all IPv6 ACLs on a device that has a single IPv6 ACL:

```
switch# show ipv6 access-lists
IPv6 access list ipv6-main-filter
        10 permit ipv6 any any
```

This example shows how to use the **show ipv6 access-lists** command to display an IPv6 ACL named ipv6-RandD-outbound-web, including per-entry statistics for the entries except for the LowerLab object group:

```
switch# show ipv6 access-lists ipv6-RandD-outbound-web
IPv6 access list ipv6-RandD-outbound-web
        statistics per-entry
        fragments deny-all
        1000 permit ahp any any [match=732]
        1005 permit tcp addrgroup LowerLab any eq telnet
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show ipv6 access-lists** command to display an IPv6 ACL named ipv6-RandD-outbound-web. The **expanded** keyword causes the contents of the object group from the previous example to appear, including the per-entry statistics:

```
switch# show ipv6 access-lists ipv6-RandD-outbound-web expanded
IPv6 access list ipv6-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp 2001:db8:0:3ab0::1/128 any eq telnet [match=5032]
        1005 permit tcp 2001:db8:0:3ab0::32/128 any eq telnet [match=433]
        1010 permit tcp any any eq www [match=820421]
```

This example shows how to use the **show ipv6 access-lists** command with the **summary** keyword to display information about an IPv6 ACL named ipv6-RandD-outbound-web, such as which interfaces the ACL is applied to and active on:

```
switch# show ipv6 access-lists ipv6-RandD-outbound-web summary
IPV6 ACL ipv6-RandD-outbound-web
        Statistics enabled
```

```
Total ACEs Configured: 4
Configured on interfaces:
        Ethernet2/4 - ingress (Router ACL)
Active on interfaces:
        Ethernet2/4 - ingress (Router ACL)
```

Related Commands

Command	Description
fragments	Configures how an IP ACL processes noninitial fragments.
ipv6 access-list	Configures an IPv6 ACL.
show access-lists	Displays all ACLs or a specific ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.
statistics per-entry	Starts recording statistics for packets permitted or denied by each entry in an ACL.

show ipv6 dhcp relay

To display the DHCPv6 relay global or interface-level configuration, including DHCPv6 server addresses configured on interfaces, use the **show ipv6 dhcp relay** command.

show ipv6 dhcp relay [**interface** *interface*]

Syntax Description

interface*interface*	(Optional) Displays the DHCPv6 relay address of the interface. The supported interface types are ethernet, port-channel, and VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the globally configured DHCPv6 relay status and DHCPv6 server addresses:

```
switch# show ipv6 dhcp relay
DHCPv6 relay service : Enabled
Insertion of VPN options : Disabled
Insertion of CISCO options : Disabled
DHCPv6 Relay is configured on the following interfaces:
Interface        Relay Address     VRF Name
 -------------    -------------     --------
 Ethernet1/4          red
```

Related Commands

Command	Description
ipv6 dhcp relay	Enables the DHCPv6 relay agent.
show ipv6 dhcp relay statistics	Displays statistics relating to DHCPv6.

show ipv6 dhcp relay statistics

To display the DHCPv6 relay statistics, use the **show ipv6 dhcp relay** statistics command.

show ipv6 dhcp relay statistics [**interface** *interface*]

Syntax Description

interface *interface*	(Optional) Displays the DHCPv6 relay address of the interface. The supported interface types are ethernet, port-channel, and VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the globally configured DHCPv6 relay statistics:

```
switch# show ipv6 dhcp relay statistics
```

Related Commands

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

show ipv6 dhcp-ldra

To display configuration details and statistics for the Lightweight DHCPv6 Relay Agent (LDRA), use the show **ipv6 dhcp-ldra** command.

show ipv6 dhcp-ldra [statistics]

Syntax Description

statistics	(Optional) Displays LDRA-related statistics.

Command Default

None

Command Modes

Any command mode

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)# show ipv6 dhcp-ldra statistics
    DHCPv6 LDRA client facing statistics.
Messages received             2
Messages sent                 2
Messages discarded            0
Messages Received
SOLICIT                       1
REQUEST                       1
Messages Sent
RELAY-FORWARD                 2
    DHCPv6 LDRA server facing statistics.
Messages received             2
Messages sent                 2
Messages discarded            0
Messages Received
RELAY-REPLY                   2
Messages Sent
ADVERTISE                     1
REPLY                         1
```

Related Commands

Command	Description
ipv6 dhcp-ldra	Enables the LDRA feature.

show ipv6 dhcp guard policy

To display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard information, use the **show ipv6 dhcp guard policy** command.

show ipv6 dhcp guard policy [*policy-name*]

Syntax Description

policy-name	(Optional) DHCPv6 guard policy name.

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

If the *policy-name* argument is specified, only the specified policy information is displayed. If the *policy-name* argument is not specified, information is displayed for all policies.

Examples

The following is sample output:

```
switch# show ipv6 dhcp guard policy

Dhcp guard policy: default
        Device Role: dhcp client
        Target: Et0/3

Dhcp guard policy: test1
        Device Role: dhcp server
        Target: vlan 0    vlan 1    vlan 2    vlan 3    vlan 4
        Max Preference: 200
        Min Preference: 0
        Source Address Match Access List: acl1
        Prefix List Match Prefix List: pfxlist1

Dhcp guard policy: test2
        Device Role: dhcp relay
        Target: Et0/0 Et0/1 Et0/2
```

The table below describes the significant fields shown in the display.

Table 1: show ipv6 dhcp guard policy

Field	Description
Device Role	The role of the device. The role is either client, server or relay.

Field	Description
Target	The name of the target. The target is either an interface or a VLAN.

show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all interfaces configured with the RA guard feature, use the **show ipv6 nd raguard policy** command.

show ipv6 nd raguard policy [*policy-name*]

Syntax Description

policy-name	(Optional) RA guard policy name.

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **show ipv6 nd raguard policy** command displays the options configured for the policy on all interfaces configured with the RA guard feature.

Examples

The following example shows the policy configuration for a policy named raguard1 and all the interfaces where the policy is applied:

```
switch# show ipv6 nd raguard policy interface raguard1

Policy raguard1 configuration:
  device-role host
Policy applied on the following interfaces:
  Et0/0        vlan all
  Et1/0        vlan all
```

The table below describes the significant fields shown in the display.

Table 2: show ipv6 nd raguard policy Field Descriptions

Field	Description
Policy raguard1 configuration:	Configuration of the specified policy.
device-role host	The role of the device attached to the port. This device configuration is that of host.
Policy applied on the following interfaces:	The specified interface on which the RA guard feature is configured.

show ipv6 neighbor binding

To display contents of a binding table, use the **show ipv6 neighbor binding** command.

show ipv6 neighbor binding[**vlan***vlan-id*| **interface***type number*| **ipv6***ipv6-address*| **mac***mac-address*]

Syntax Description

vlan *vlan-id*	(Optional) Displays the binding table entries that match the specified VLAN.
interface *type number*	(Optional) Displays the binding table entries that match the specified interface type and number.
ipv6 *ipv6-address*	(Optional) Displays the binding table entries that match the specified IPv6 address.
mac *mac-address*	(Optional) Displays the binding table entries that match the specified Media Access Control (MAC) address.

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

This command displays the contents of the binding table. The display output can be specified by the specified VLAN, interface, IPv6 address, or MAC address. If no keywords or arguments are entered, all binding table contents are displayed.

Examples

The following example displays the contents of a binding table:

```
switch# show ipv6 neighbor binding

address DB has 4 entries
Codes: L - Local, S - Static, ND - Neighbor Discovery
Preflevel (prlvl) values:
1:Not secure          2:MAC and LLA match   3:Cga authenticated
4:Dhcp assigned       5:Cert authenticated  6:Cga and Cert auth
7:Trusted port        8:Statically assigned
    IPv6 address            Link-Layer addr Interface   vlan  prlvl age state    Time left
ND  FE80::A8BB:CCFF:FE01:F500  AABB.CC01.F500  Et0/0     100  0002    0 REACHABLE  8850
L   FE80::21D:71FF:FE99:4900   001D.7199.4900  Vl100     100  0080 7203 DOWN       N/A
ND  2001:600::1                AABB.CC01.F500  Et0/0     100  0003    0 REACHABLE  3181
ND  2001:300::1                AABB.CC01.F500  Et0/0     100  0007    0 REACHABLE  9559
ND  2001:100::2                AABB.CC01.F600  Et1/0     200  0002    0 REACHABLE  9196
```

```
L   2001:400::1                001D.7199.4900  Vl100     100  0080 7188 DOWN       N/A
S   2001:500::1                000A.000B.000C  Fa4/13    300  0080 8676 STALE      N/A
```

The table below describes the significant fields shown in the display.

Table 3: show ipv6 neighbor binding Field Descriptions

Field	Description
address DB has *n* entries	Number of entries in the specified database.

show ipv6 snooping capture-policy

To display message capture policies, use the **show ipv6 snooping capture-policy** command.

show ipv6 snooping capture-policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first-hop message types on the specified interface type and number.

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **show ipv6 snooping capture-policy** command displays IPv6 first-hop message capture policies.

Examples

The following example shows **show ipv6 snooping capture-policy** command output on the Ethernet 0/0 interface, on which the IPv6 Neighbor Discovery Protocol (NDP) Inspection and Router Advertisement (RA) Guard features are configured:

```
switch# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol  Protocol value  Message  Value  Action  Feature
ICMP      58              RS       85     punt    RA Guard
                                          punt    ND Inspection
ICMP      58              RA       86     drop    RA guard
                                          punt    ND Inspection
ICMP      58              NS       87     punt    ND Inspection
ICMP      58              NA       88     punt    ND Inspection
ICMP      58              REDIR    89     drop    RA Guard
                                          punt    ND Inspection
```

The table below describes the significant fields shown in the display.

Table 4: show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.

Field	Description
Message	The type of message being inspected.
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

To display information about the packets counted by the interface counter, use the **show ipv6 snooping counters**command.

show ipv6 snooping counters {**interface** *type number*| **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays first-hop packets that match the specified interface type and number.
vlan *vlan-id*	Displays first-hop packets that match the specified VLAN ID.

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **show ipv6 snooping counters** command displays packets handled by the switch that are being counted in interface counters. The switch counts packets captured per interface and records whether the packet was received, sent, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples shows information about packets counted on Fast Ethernet interface 4/12:

```
switch# show ipv6 snooping counters interface Fa4/12
Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4256    0       0       0       0       0
Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4240    0       0       0       0       0
Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0
Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

The table below describes the significant fields shown in the display.

Table 5: show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from:	Bridged messages from the interface.
Dropped messages on:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:	The reason that these messages were dropped.

show ipv6 snooping features

To display information about about snooping features configured on the router, use the **show ipv6 snooping features** command.

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **show ipv6 snooping features** command displays the first-hop features that are configured on the router.

Examples

The following example shows that both IPv6 NDP inspection and IPv6 RA guard are configured on the router:

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

The table below describes the significant fields shown in the display.

Table 6: show ipv6 snooping features Field Descriptions

Field	Description
Feature name	The names of the IPv6 global policy features configured on the router.
priority	The priority of the specified feature.
state	The state of the specified feature.

show ipv6 snooping policies

To display information about the configured policies and the interfaces to which they are attached, use the **show ipv6 snooping policies** command.

show ipv6 snooping policies {**interface** *type number*| **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays policies that match the specified interface type and number.
vlan *vlan-id*	Displays first-hop packets that match the specified VLAN ID.

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **show ipv6 snooping policies** command displays all policies that are configured and lists the interfaces to which they are attached.

Examples

The following example shows information about all policies configured:

```
switch# show ipv6 snooping policies

NDP inspection policies configured:
Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all
RA guard policies configured:
Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```

The table below describes the significant fields shown in the display.

Table 7: show ipv6 snooping policies Field Descriptions

Field	Description
NDP inspection policies configured:	Description of the policies configured for a specific feature.
Policy	Whether the policy is trusted or untrusted.
Interface	The interface to which a policy is attached.

show key chain

To display the configuration for a specific keychain, use the **show key chain** command.

show key chain [*keychain-name* | **mode decrypt**]

Syntax Description

keychain-name	(Optional) Name of the keychain that is configured, up to 63 alphanumerical characters.
mode decrypt	(Optional) Shows the key text configuration in cleartext. This option is available only when the device is accessed with a user account that is assigned a network-admin or vdc-admin user role.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
8.2(1)	This command was modified to display the details of the MACsec keychains configured.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the keychain configuration for the glbp-key keychain that contains one key (key 13) with specific accept and send lifetimes:

```
switch# show key chain
Key-Chain glbp-keys
  Key 13 -- text 7 071a33595c1d0c1702170203163e3e21213c20361a021f11
    accept lifetime UTC (00:00:00 Jun 13 2008) - (23:59:59 Sep 12 2008)
    send lifetime UTC (00:00:00 Jun 13 2008) - (23:59:59 Aug 12 2008)
```

This example shows how to display the MACsec keychain configuration for the k1 MACsec keychain that contains the 01 MACsec key:

```
switch# show key chain k1
Key-Chain k1 Macsec
  Key 01 -- text 7 "075f701e1d5d4c53404a520d052829272b6364704053435556 0e005952560c001b"
```

```
cryptographic-algorithm AES_128_CMAC
send lifetime (always valid) [active]
```

Related Commands

Command	Description
accept-lifetime	Configures an accept lifetime for a key.
key	Configures a key.
key chain	Configures a keychain.
key-octet-string	Configures the text for a MACsec key.
key-string	Configures a key string.
send-lifetime	Configures a send lifetime for a key.

show ldap-search-map

To display information about the configured Lightweight Directory Access Protocol (LDAP) attribute maps, use the **show ldap**-search-map command.

show ldap-search-map

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display information about the configured LDAP attribute maps:

```
switch# show ldap-search-map
total number of search maps : 1
following LDAP search maps are configured:
    SEARCH MAP  s0:
      User Profile:
        BaseDN: DN1
        Attribute Name: map1
        Search Filter: filter1
```

Related Commands

Command	Description
attribute-name	Configures the attribute name, search filter, and base-DN for the user profile, trusted certificate, CRL, certificate DN match, public key match, or user-switchgroup lookup search operation.
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.

Command	Description
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.

show ldap-server

To display the Lightweight Directory Access Protocol (LDAP) server configuration, use the **show ldap-server** command.

show ldap-server

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display the LDAP server configuration:

```
switch# show ldap-server
  timeout : 5
        port : 389
    deadtime : 0
total number of servers : 0
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.

show ldap-server groups

To display the Lightweight Directory Access Protocol (LDAP) server group configuration, use the **show ldap-server groups** command.

show ldap-server groups

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display the LDAP server group configuration:

```
switch# show ldap-server groups
total number of groups: 1
following LDAP server groups are configured:
    group LDAPgroup1:
        Use-vrf: default
        Mode: UnSecure
        Authentication: Search and Bind
        Bind and Search : append with basedn (cn=$userid)
        Authentication: Do bind instead of compare
        Bind and Search : compare passwd attribute userPassword
        Authentication Mech: Default(PLAIN)
        Search map:
```

Related Commands

Command	Description
aaa group server ldap	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.
feature ldap	Enables LDAP.

show ldap-server statistics

To display the Lightweight Directory Access Protocol (LDAP) server statistics, use the **show ldap-server statistics** command.

show ldap-server statistics {*ipv4-address*| *ipv6-address*| *host-name*}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X:X* format.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display the statistics for an LDAP server:

```
switch# show ldap-server statistics 10.10.1.1
Server is not monitored
Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

Related Commands

Command	Description
feature ldap	Enables LDAP.

Command	Description
ldap-server host	Specifies the IPv4 or IPv6 address or hostname for an LDAP server.

show mac access-lists

To display all MAC access control lists (ACLs) or a specific MAC ACL, use the **show mac access-lists** command.

show mac access-lists [*access-list-name*] [**expanded**| **summary**]

Syntax Description

access-list-name	(Optional) Name of a MAC ACL, which can be up to 64 alphanumeric, case-sensitive characters.
expanded	(Optional) Specifies that the contents of object groups show rather than the names of object groups only.
summary	(Optional) Specifies that the command displays information about the ACL rather than the ACL configuration. For more information, see the “Usage Guidelines” section.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names.
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all MAC ACLs, unless you use the *access-list-name* argument to specify an ACL.

If you do not specify an ACL name, the device lists ACLs alphabetically by the ACL names.

The **expanded** keyword allows you to display the details of object groups used in an ACL rather than only the name of the object groups. For more information about object groups, see the **object-group ip address**, **object-group ipv6 address**, and **object-group ip port** commands.

The **summary** keyword allows you to display information about the ACL rather than the ACL configuration. The information displayed includes the following:

- Whether per-entry statistics are configured for the ACL.
- The number of rules in the ACL configuration. This number does not reflect how many entries that the ACL contains when the device applies it to an interface. If a rule in the ACL uses an object group, the number of entries in the ACL when it is applied may be much greater than the number of rules.

- The interfaces that the ACL is applied to.
- The interfaces that the ACL is active on.

The **show mac access-lists** command displays statistics for each entry in an ACL if the following conditions are both true:

- The ACL configuration contains the **statistics per-entry** command.
- The ACL is applied to an interface that is administratively up.

This command does not require a license.

Examples

This example shows how to use the **show mac access-lists** command to show all MAC ACLs on a device with a single MAC ACL:

```
switch# show mac access-lists
MAC access list mac-filter
        10 permit any any ip
```

This example shows how to use the **show mac access-lists** command to display a MAC ACL named mac-lab-filter, including per-entry statistics:

```
switch# show mac access-lists mac-lab-filter
MAC access list mac-lab-filter
        statistics per-entry
        10 permit 0600.ea5f.22ff 0000.0000.0000 any [match=820421]
        20 permit 0600.050b.3ee3 0000.0000.0000 any [match=732]
```

This example shows how to use the **show mac access-lists** command with the **summary** keyword to display information about a MAC ACL named mac-lab-filter, such as which interfaces the ACL is applied to and active on:

```
switch# show mac access-lists mac-lab-filter summary
MAC ACL mac-lab-filter
        Statistics enabled
        Total ACEs Configured: 2
        Configured on interfaces:
                Ethernet2/3 - ingress (Port ACL)
        Active on interfaces:
                Ethernet2/3 - ingress (Port ACL)
```

Related Commands

Command	Description
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show ipv6 access-lists	Displays all IPv6 ACLs or a specific IPv6 ACL.

show macsec mka

To display the details of MACsec Key Agreement (MKA), use the **show macsec mka** command.

show macsec mka [**capability interface** {**all** | **ethernet** *slot-number*/*port-number*}| **session** [**interface ethernet** *slot*/*port*][**details**] [**internal-details**] | **statistics** [**interface ethernet** *slot*/*port*] | **summary**]

Syntax Description

capability interface	(Optional) Shows the capability of MKA in the interfaces.
all	Shows the capability of all the interfaces.
ethernet *slot*/*port*	Shows capability of the specified Ethernet interface.
session	(Optional) Shows MKA session information.
interface ethernet *slot*/*port*	(Optional) Shows information about the specified Ethernet interface.
details	(Optional) Shows detailed information about MKA.
internal-details	(Optional) Shows internal detailed information about MKA.
statistics	(Optional) Shows MKA statistics.
summary	(Optional) Shows MKA summary information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the details of an MKA session:

```
switch# show macsec mka session details

Detailed Status for MKA Session
-----------------------------------
Interface Name          : Ethernet11/25
Session Status                      : Secured
Local Tx-SCI                        : 00b0.e135.9c24/0001
Local Tx-SSCI                       : 3
MKA Port Identifier                 : 3
CAK Name (CKN)                      :
0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)              : 17173194E288E086B275A49F
Message Number (MN)                 : 12465
MKA Policy Name                     : p1
Key Server Priority                 : 9
Key Server                          : No
SAK Cipher Suite                    : GCM-AES-XPN-128
SAK Cipher Suite (Operational)      : GCM-AES-XPN-128
Replay Window Size                  : 0
Confidentiality Offset              : CONF-OFFSET-0
Confidentiality Offset (Operational): CONF-OFFSET-0
Latest SAK Status                   : Rx & TX
Latest SAK AN                       : 0
Latest SAK KI                       : 10314879
Latest SAK KN                       : 57
Last SAK key time                   : 06:59:24 UTC Wed Apr 19 2017
Number of Macsec Capable Live Peers: 3
Number of SA consumed in Hardware  : 3
Number of Macsec Capable Live Peers Responded: 0
Live Peer List:
MI                        MN        SCI                SSCI Key-Server Priority
-----------------------------------------------------------------------------------------
7F649D00075CA2B14065F50D  12466      00b0.e135.9c23/0001 4     9
67DF7F5DE06AFC9A2F125914  12464      9c57.adfd.8acb/0001 2     9
57BCB803EB00453525F7382C  12466      9c57.adfd.8acc/0001 1     9

Detailed Status for MKA Session
-----------------------------------
Interface Name          : Ethernet4/27
    Session Status                      : Secured
    Local Tx-SCI                        : 5006.ab91.9f4e/0001
    Local Tx-SSCI                       : 2
    MKA Port Identifier                 : 2
    CAK Name (CKN)                      :
1000000000000000000000000000000000000000000000000000000000000000
    Member Identifier (MI)              : 4B18586C685B28F2354B1E2B
    Message Number (MN)                 : 49
    MKA Policy Name                     : mustsecureks
    Key Server Priority                 : 9
    Key Server                          : Yes
    SAK Cipher Suite                    : GCM-AES-256
    SAK Cipher Suite (Operational)      : GCM-AES-256
    Replay Window Size                  : 0
    Confidentiality Offset              : CONF-OFFSET-0
    Confidentiality Offset (Operational): CONF-OFFSET-0
    Latest SAK Status                   : Rx & TX
    Latest SAK AN                       : 2
    Latest SAK KI                       : 1817712715
    Latest SAK KN                       : 1
    Last SAK key time                   : 20:42:51 UTC Thu May 04 2017
    Number of Macsec Capable Live Peers: 2
    Number of SA consumed in Hardware  : 2
    Number of Macsec Capable Live Peers Responded: 2
Live Peer List:
MI                        MN        SCI                SSCI Key-Server-Priority Tx/Rx
Programmed
-------------------------------------------------------------------------------
```

```
----------------
3634B7ADE028833E219C2304  7624       9c57.adfc.0f34/0001 1     16                    Yes
92D6F93C2BC4058AD25FA0E5  7655       5006.ab91.4584/0001 3     16                    Yes
```

This example shows how to display the MKA statistics for a specified interface:

```
switch#  show macsec mka statistics interface ethernet 11/25

Per-CA MKA Statistics for Session on interface (Ethernet11/25) with CKN 0x1
============================================================================
CA Statistics
   Pairwise CAK Rekeys..... 0

SA Statistics
   SAKs Generated.......... 0
   SAKs Rekeyed............ 0
   SAKs Received........... 60
   SAK Responses Received.. 0

MKPDU Statistics
   MKPDUs Transmitted...... 18676
      "Distributed SAK".. 0

   MKPDUs Validated & Rx... 55986
      "Distributed SAK".. 60

MKA Statistics for Session on interface (Ethernet11/25)
=======================================================
CA Statistics
   Pairwise CAK Rekeys..... 0

SA Statistics
   SAKs Generated.......... 0
   SAKs Rekeyed............ 0
   SAKs Received........... 60
   SAK Responses Received.. 0

MKPDU Statistics
   MKPDUs Transmitted...... 18676
      "Distributed SAK".. 0
   MKPDUs Validated & Rx... 55986
      "Distributed SAK".. 60

MKA IDB Statistics
   MKPDUs Tx Success.......... 19147
   MKPDUs Tx Fail............. 0
   MKPDUS Tx Pkt build fail... 0
   MKPDUS No Tx on intf down.. 0
   MKPDUS No Rx on intf down.. 0
   MKPDUs Rx CA Not found..... 0
   MKPDUs Rx Error............ 0
   MKPDUs Rx Success.......... 55986

MKPDU Failures
   MKPDU Rx Validation ..................... 0
   MKPDU Rx Bad Peer MN..................... 0
   MKPDU Rx Non-recent Peerlist MN.......... 0
   MKPDU Rx Drop SAKUSE, KN mismatch........ 0
   MKPDU Rx Drop SAKUSE, Rx Not Set......... 0
   MKPDU Rx Drop SAKUSE, Key MI mismatch.... 0
   MKPDU Rx Drop SAKUSE, AN Not in Use...... 0
   MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set... 16956
   MKPDU Rx Drop Packet, Ethertype Mismatch. 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0

CA Failures
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SA Installation.............. 12
   Tx SA Installation.............. 0
```

This example shows how to display the MKA summary:

```
switch# show macsec mka summary

Interface      Status   Cipher           Key-Server   MACSEC-policy  CKN
                                            Keychain
-------------- -------- ---------------- ------------ --------------
---------------------------------------------------------------- ---------
Ethernet11/25  Secured  GCM-AES-XPN-128  No           p1
0100000000000000000000000000000000000000000000000000000000000000 k1
Ethernet11/31  Secured  GCM-AES-XPN-128  Yes          p1
0300000000000000000000000000000000000000000000000000000000000000 k3
```

Related Commands

Command	Description
cipher suite	Configures the cipher suite for encrypting traffic with MACsec.
conf-offset	Configures the confidentiality offset for MKA encryption.
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
key-octet-string	Configures the text for a MACsec key.
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
sak-expiry-time *time*	Sets an expiry time for a force SAK rekey.
show key chain	Displays the configuration of the specified keychain.
show macsec policy	Displays all the MACsec policies in the system.
show run mka	Displays the status of MKA.

show macsec policy

To display the details of the MACsec policies, use the **show macsec policy** command.

show macsec policy [*policy-name*]

Syntax Description

policy-name	(Optional) Name of the MACsec policy.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the details of all the MACsec policies:

```
switch# show macsec policy
MACsec Policy                    Cipher           Pri  Window   Offset   Security     SAK
Rekey time
-------------------------------- ---------------- ---- -------- -------- ------------
--------------
p1                               GCM-AES-XPN-128  9    0        0        must-secure  60

system-default-macsec-policy     GCM-AES-XPN-256  16   0        0        must-secure
pn-exhaust
```

This example shows how to display the details of the user-defined MACsec policy:

```
switch# show macsec policy p1
MACsec Policy                    Cipher           Pri  Window   Offset   Security     SAK
Rekey time
-------------------------------- ---------------- ---- -------- -------- ------------
--------------
p1                               GCM-AES-XPN-128  9    0        0        must-secure  60
```

Related Commands

Command	Description
cipher suite	Configures the cipher suite for encrypting traffic with MACsec.

Command	Description
conf-offset	Configures the confidentiality offset for MKA encryption.
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
key-octet-string	Configures the text for a MACsec key.
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
sak-expiry-time *time*	Sets an expiry time for a force SAK rekey.
show key chain	Displays the configuration of the specified keychain.
show macsec mka	Displays the details of MKA.
show run mka	Displays the status of MKA.

show password secure-mode

To display the secure mode for changing password, use the **show password secure-mode** command.

show password secure-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Any command mode

Command History

Release	Modification
6.1.4	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the secure mode for changing password:

```
switch# show password secure-mode
Password secure mode is enabled
```

Related Commands

Command	Description
password strength-check	Enables password-strength checking.

show password strength-check

To display password-strength checking status, use the **show password strength-check** command.

show password strength-check

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display password-strength checking status:

```
switch# show password strength-check
Password strength check enabled
```

Related Commands

Command	Description
password strength-check	Enables password-strength checking.
show running-config security	Displays security feature configuration in the running configuration.

show policy-map interface control-plane

To display packet-level statistics for all classes that are part of the applied control plane policing (CoPP) policy, use the **show policy-map interface control-plane** command.

show policy-map interface control-plane {[**module** *module-number* **[inst-all]**] [**class** {*class-name*| **violated**}]| [**class** {*class-name*| **violated**}] [**module** *module-number* **[inst-all]**]}

Syntax Description

class *class-name*	Displays the packet-level statistics for the specific class.
module *module-number*	Displays the packet-level statistics for the specific module. The range is from 1 to 18.
violated	Displays classes that have violated the police rate.
inst-all	Displays per-instance statistics.

Command Modes

Any command mode

Command History

Release	Modification
8.1(1)	Added the **inst-all** keyword.
6.2(2)	This command was introduced.

Usage Guidelines

Use this command to display the policy values with associated class maps and drops per policy or class map. It also displays the scale factor values when a CoPP policy is applied. When the scale factor value is the default (1.00), it is not displayed.

Note The scale factor changes the CIR, BC, PIR, and BE values internally on each module, but the display shows the configured CIR, BC, PIR, and BE values only. The actual applied value on a module is the scale factor multiplied by the configured value.

This command does not require a license.

Examples

This example shows how to monitor CoPP:

```
switch# show policy-map interface control-plane
Control Plane
service-policy input: copp-system-policy-default
```

```
class-map copp-system-class-igmp (match-any)
match protocol igmp
police cir 1024 kbps , bc 65535 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
class-map copp-system-class-pim-hello (match-any)
match protocol pim
police cir 1024 kbps , bc 4800000 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
....
```

This example shows the 5-minute moving averages and peaks of the conformed and violated byte counts in the output of the show policy-map interface control-plane command. In this example, the 5-minute offered rate is the 5-minute moving average of the conformed bytes, the 5-minute violate rate is the 5-minute moving average of the violated bytes, and the peak rate is the highest value since bootup or counter reset, with the peak occurring at the time stamp shown.

```
module 9:
  conformed 0 bytes,
    5-min offered rate 10 bytes/sec
    peak rate 12 bytes/sec at 12:29:38.654 UTC Sun Jun 30 2013
  violated 0 bytes,
   5-min violate rate 20 bytes/sec
   peak rate 22 bytes/sec at 12:26:22.652 UTC Sun Jun 30 2013
```

This example displays the per-instance statistics for all classes that are part of the applied control plane policing (CoPP) policy for a module.

```
switch(config)# show policy-map interface control-plane module 9 inst-all
Control Plane
  service-policy input copp-system-p-policy-strict

    class-map copp-system-p-class-critical (match-any)
      match access-group name copp-system-p-acl-bgp
      match access-group name copp-system-p-acl-rip
      match access-group name copp-system-p-acl-vpc
      match access-group name copp-system-p-acl-bgp6
      match access-group name copp-system-p-acl-lisp
      match access-group name copp-system-p-acl-ospf
      match access-group name copp-system-p-acl-rip6
      match access-group name copp-system-p-acl-rise
      match access-group name copp-system-p-acl-eigrp
      match access-group name copp-system-p-acl-lisp6
      match access-group name copp-system-p-acl-ospf6
      match access-group name copp-system-p-acl-rise6
      match access-group name copp-system-p-acl-eigrp6
      match access-group name copp-system-p-acl-otv-as
      match access-group name copp-system-p-acl-mac-l2pt
      match access-group name copp-system-p-acl-mpls-ldp
      match access-group name copp-system-p-acl-mpls-rsvp
      match access-group name copp-system-p-acl-mac-l3-isis
      match access-group name copp-system-p-acl-mac-otv-isis
      match access-group name copp-system-p-acl-mac-fabricpath-isis
      match protocol mpls router-alert
      set cos 7
      police cir 36000 kbps bc 250 ms
        conform action: transmit
        violate action: drop
      module 9:
      inst 0:
        conformed 3215360 bytes,
          5-min offered rate 7 bytes/sec
          peak rate 9 bytes/sec at Fri Apr 28 11:58:48 2017
      inst 1:
        conformed 3210508 bytes,
          5-min offered rate 7 bytes/sec
          peak rate 8 bytes/sec at Wed May 03 05:19:24 2017
      inst 2:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 3:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 4:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 5:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 0:
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 1:
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 2:
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 3:
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 4:
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 5:
        violated 0 bytes,
          5-min violate rate 0 bytes/sec
          peak rate 0 bytes/sec

    class-map copp-system-p-class-important (match-any)
      match access-group name copp-system-p-acl-cts
      match access-group name copp-system-p-acl-glbp
      match access-group name copp-system-p-acl-hsrp
      match access-group name copp-system-p-acl-vrrp
      match access-group name copp-system-p-acl-wccp
      match access-group name copp-system-p-acl-hsrp6
      match access-group name copp-system-p-acl-vrrp6
      match access-group name copp-system-p-acl-opflex
      match access-group name copp-system-p-acl-mac-lldp
      match access-group name copp-system-p-acl-mac-mvrp
      match access-group name copp-system-p-acl-mac-flow-control
      set cos 6
      police cir 1400 kbps bc 1500 ms
        conform action: transmit
        violate action: drop
      module 9:
      inst 0:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 1:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
      inst 2:
        conformed 0 bytes,
          5-min offered rate 0 bytes/sec
          peak rate 0 bytes/sec
```

Related Commands

Command	Description
show copp status	Displays the CoPP status, including the last configuration operation and its status.

show policy-map type control-plane

To display control plane policy map information, use the **show policy-map type control-plane** command.

show policy-map type control-plane [expand] [**name** *policy-map-name*]

Syntax Description

expand	(Optional) Displays expanded control plane policy map information.
name *policy-map-name*	(Optional) Specifies the name of the control plane policy map. The name is case sensitive.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display control plane policy map information:

```
switch# show policy-map type control-plane
  policy-map type control-plane copp-system-policy
    class copp-system-class-critical
      police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class copp-system-class-important
      police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class copp-system-class-normal
      police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class class-default
      police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
```

show port-security

To show the state of port security on the device, use the **show port-security** command.

show port-security [state]

Syntax Description

state	(Optional) Shows that port security is enabled.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to use the **show port-security** command to view the status of the port security feature on a device:

```
switch# show port-security
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
----------------------------------------------------------------------------
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
----------------------------------------------------------------------------
Ethernet1/4           5              1              0              Shutdown
============================================================================
switch#
```

Related Commands

Command	Description
feature port-security	Enables the port security feature.
show port-security address	Shows MAC addresses secured by the port security feature.
show port-security interface	Shows the port security status for a specific interface.

Command	Description
switchport port-security	Configures port security on a Layer 2 interface.

show port-security address

To show information about MAC addresses secured by the port security feature, use the **show port-security address** command.

show port-security address [**interface** {**port-channel** *channel-number*| **ethernet** *slot/port*}]

Syntax Description

interface	(Optional) Limits the port-security MAC address information to a specific interface.
port-channel *channel-number*	Specifies a Layer 2 port-channel interface. The *channel-number* argument can be a whole number from 1 to 4096.
ethernet*slot/port*	Specifies an Ethernet interface.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to use the **show port-security address** command to view information about all MAC addresses secured by port security:

```
switch# show port-security address
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
----------------------------------------------------------------------
                    Secure Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining Age
                                                              (mins)
----    -----------            ------           -----     -------------
   1    0054.AAB3.770F         STATIC       port-channel1     0
   1    00EE.378A.ABCE         STATIC       Ethernet1/4       0
======================================================================
switch#
```

This example shows how to use the **show port-security address** command to view the MAC addresses secured by the port security feature on the Ethernet 1/4 interface:

```
switch# show port-security address interface ethernet 1/4
                     Secure Mac Address Table
----------------------------------------------------------------------
Vlan    Mac Address             Type             Ports      Remaining Age
                                                              (mins)
----    -----------            ------            -----     -------------
   1    00EE.378A.ABCE         STATIC        Ethernet1/4       0
----------------------------------------------------------------------
switch#
```

Related Commands

Command	Description
feature port-security	Enables the port security feature.
show port-security	Shows the status of the port security feature.
show port-security interface	Shows the port security status for a specific interface.
switchport port-security	Configures port security on a Layer 2 interface.

show port-security interface

To show the state of port security on a specific interface, use the **show port-security interface** command.

show port-security interface {**port-channel** *channel-number*| **ethernet** *slot/port*}

Syntax Description

port-channel *channel-number*	Specifies a Layer 2 port-channel interface. The *channel-number* argument can be a whole number from 1 to 4096.
ethernet*slot/port*	Specifies an Ethernet interface.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Support for Layer 2 port-channel interfaces was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to use the **show port-security interface** command to view the status of the port security feature on the Ethernet 1/4 interface:

```
switch# show port-security interface ethernet 1/4
Port Security              : Enabled
Port Status                : Secure Down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
Maximum MAC Addresses      : 5
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Security violation count   : 0
switch#
```

Related Commands

Command	Description
feature port-security	Enables the port security feature.
show port-security	Shows the status of the port security feature.
show port-security address	Shows MAC addresses secured by the port security feature.
switchport port-security	Configures port security on a Layer 2 interface.

show privilege

To show the current privilege level, username, and status of cumulative privilege support, use the **show** privileg**e** command.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 use the **show privilege** command to view the current privilege level, username, and status of cumulative privilege support:

```
switch# show privilege
User name: admin
Current privilege level: -1
Feature privilege: Enabled
switch#
```

Related Commands

Command	Description
enable *level*	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
username *username* **priv-lvl**	Enables a user to use privilege levels for authorization.

show radius

To display the RADIUS Cisco Fabric Services (CFS) distribution status and other details, use the **show radius** command.

show radius {**distribution status**| **merge status**| **pending [cmds]**| **pending-diff**| **session status**| **status**}

Syntax Description

distribution status	Displays the status of the RADIUS CFS distribution.
merge status	Displays the status of a RADIUS merge.
pending	Displays the pending configuration that is not yet applied to the running configuration.
cmds	(Optional) Displays the commands for the pending configuration.
pending-diff	Displays the difference between the active configuration and the pending configuration.
session status	Displays the status of the RADIUS CFS session.
status	Displays the status of the RADIUS CFS.

Command Default

None

Command Modes

Any command mode

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 display the RADIUS CFS distribution status:

```
switch# show radius distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: not yet initiated after enable
```

```
last operation: enable
last operation status: success
```

This example shows how to display the RADIUS merge status:

```
switch# show radius merge status
Result: Waiting
```

This example shows how to display the RADIUS CFS session status:

```
switch# show radius session status
Last Action Time Stamp     : None
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
```

This example shows how to display the RADIUS CFS status:

```
switch# show radius status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: not yet initiated after enable
last operation: enable
last operation status: success
```

This example shows how to display the pending RADIUS configuration:

```
switch# show radius pending
radius-server host 10.10.1.1 key 7 qxz123aaa group server radius aaa-private-sg
```

This example shows how to display the pending RADIUS configuration commands:

```
switch# show radius pending cmds
radius-server host 10.10.1.1 key 7 qxz12345 auth_port 1812 acct_port 1813 authentication
accounting
```

This example shows how to display the differences between the pending RADIUS configuration and the current RADIUS configuration:

```
switch(config)# show radius pending-diff
    +radius-server host 10.10.1.1 authentication accounting
```

show radius-server

To display RADIUS server information, use the **show radius-server** command.

show radius-server [*hostname*| *ipv4-address*| **ipv6-address**] [**directed-request**| **groups**| **sorted**| **statistics**]

Syntax Description

hostname	(Optional) RADIUS server Domain Name Server (DNS) name. The name is case sensitive.
ipv4-address	(Optional) RADIUS server IPv4 address in the *A.B.C.D* format.
ipv6-address	(Optional) RADIUS server IPv6 address in the *X*:*X*:*X*:*X* format.
directed-request	(Optional) Displays the directed request configuration.
groups	(Optional) Displays information about the configured RADIUS server groups.
sorted	(Optional) Displays sorted-by-name information about the RADIUS servers.
statistics	(Optional) Displays RADIUS statistics for the RADIUS servers.

Command Default

Displays the global RADIUS server configuration

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

RADIUS preshared keys are not visible in the **show radius-server** command output. Use the **show running-config radius** command to display the RADIUS preshared keys.

This command does not require a license.

Examples

This example shows how to display information for all RADIUS servers:

```
switch# show radius-server
Global RADIUS shared secret:********
retransmission count:1
timeout value:5
deadtime value:0
total number of servers:2
following RADIUS servers are configured:
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
        10.10.2.2:
                available for authentication on port:1812
                available for accounting on port:1813
```

This example shows how to display information for a specified RADIUS server:

```
switch# show radius-server 10.10.1.1
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
                idle time:0
                test user:test
                test password:********
```

This example shows how to display the RADIUS directed request configuration:

```
switch# show radius-server directed-request
enabled
```

This example shows how to display information for RADIUS server groups:

```
switch# show radius-server groups
total number of groups:2
following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
        group RadServer:
                deadtime is 0
                vrf is management
```

This example shows how to display information for a specified RADIUS server group:

```
switch# show radius-server groups RadServer
        group RadServer:
                deadtime is 0
                vrf is management
```

This example shows how to display sorted information for all RADIUS servers:

```
switch# show radius-server sorted
Global RADIUS shared secret:********
retransmission count:1
timeout value:5
deadtime value:0
total number of servers:2
following RADIUS servers are configured:
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
```

This example shows how to display statistics for a specified RADIUS server:

```
switch# show radius-server statistics 10.10.1.1
Server is not monitored
```

```
Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

Related Commands

Command	Description
show running-config radius	Displays the RADIUS information in the running configuration file.

show role

To display the user role configuration, use the **show role** command.

show role [**name** *role-name*]

Syntax Description

name *role-name*	(Optional) Displays information for a specific user role name. The role name is case sensitive.

Command Default

Displays information for all user roles.

Command Modes

Any command mode

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 display information for a specific user role:

```
switch(config)# show role name MyRole
role: MyRole
  description: new role
  vlan policy: deny
  permitted vlan
  1-10
  interface policy: deny
  permitted interface
  Ethernet2/1-8
  vrf policy: permit (default)
```

This example shows how to display information for all user roles in the default virtual device context (VDC):

```
switch(config)# show role
role: network-admin
  description: Predefined network admin role has access to all commands
  on the switch
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  1       permit  read-write
role: network-operator
  description: Predefined network operator role has access to all read
  commands on the switch
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  1       permit  read
role: vdc-admin
  description: Predefined vdc admin role has access to all commands within
  a VDC instance
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  1       permit  read-write
role: vdc-operator
  description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  1       permit  read
role: MyRole
  description: new role
  vlan policy: deny
  permitted vlan
  1-10
  interface policy: deny
  permitted interface
  Ethernet2/1-8
  vrf policy: permit (default)
```

This example shows how to display information for all user roles in a nondefault virtual device context (VDC):

```
switch-MyVDC# show role
role: vdc-admin
  description: Predefined vdc admin role has access to all commands within
  a VDC instance
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  1       permit  read-write
role: vdc-operator
  description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  -------------------------------------------------------------------
  1       permit  read
```

Related Commands

Command	Description
role name	Configures user roles.

show role feature

To display the user role features, use the **show role feature** command.

show role feature [**detail**| **name** *feature-name*]

Syntax Description

detail	(Optional) Displays detailed information for all features.
name *feature-name*	(Optional) Displays detailed information for a specific feature. The feature name is case sensitive.

Command Default

Displays a list of user role feature names.

Command Modes

Any command mode

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 display the user role features:

```
switch(config)# show role feature
feature: aaa
feature: access-list
feature: arp
feature: callhome
feature: cdp
feature: crypto
feature: gold
feature: install
feature: l3vm
feature: license
feature: ping
feature: platform
feature: qosmgr
feature: radius
feature: scheduler
feature: snmp
feature: syslog
<content deleted>
```

This example shows how to display detailed information for all the user role features:

```
switch(config)# show role feature detail
```

```
feature: aaa
  show aaa *
  config t ; aaa *
  aaa *
  clear aaa *
  debug aaa *
  show accounting *
  config t ; accounting *
  accounting *
  clear accounting *
  debug accounting *
feature: access-list
  show ip access-list *
  show ipv6 access-list *
  show mac access-list *
  show arp access-list *
  show vlan access-map *
  config t ; ip access-list *
  config t ; ipv6 access-list *
  config t ; mac access-list *
  config t ; arp access-list *
  config t ; vlan access-map *
  clear ip access-list *
  clear ipv6 access-list *
  clear mac access-list *
  clear arp access-list *
  clear vlan access-map *
  debug aclmgr *
feature: arp
  show arp *
  show ip arp *
  config t; ip arp *
  clear ip arp *
  debug ip arp *
  debug-filter ip arp *
<content deleted>
```

This example shows how to display detailed information for a specific user role feature:

```
switch(config)# show role feature name dot1x
feature: dot1x
  show dot1x *
  config t ; dot1x *
  dot1x *
  clear dot1x *
  debug dot1x *
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.
rule	Configures rules for user roles.

show role feature-group

To display the user role feature groups, use the **show role feature-group** command.

show role feature-group [**detail**| **name** *group-name*]

Syntax Description

detail	(Optional) Displays detailed information for all feature groups.
name *group-name*	(Optional) Displays detailed information for a specific feature group. The group name is case sensitive.

Command Default

Displays a list of user role feature groups.

Command Modes

Any command mode

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 display the user role feature groups:

```
switch(config)# show role feature-group
feature group: L3
feature: router-bgp
feature: router-eigrp
feature: router-isis
feature: router-ospf
feature: router-rip
feature group: SecGroup
feature: aaa
feature: radius
feature: tacacs
```

This example shows how to display detailed information about all the user role feature groups:

```
switch(config)# show role feature-group detail
feature group: L3
feature: router-bgp
  show bgp *
  config t ; bgp *
  bgp *
  clear bgp *
  debug bgp *
  show ip bgp *
  show ip mbgp *
  show ipv6 bgp *
  show ipv6 mbgp *
  clear ip bgp *
  clear ip mbgp *
  debug-filter ip *
  debug-filter ip bgp *
  config t ; router bgp *
feature: router-eigrp
  show eigrp *
  config t ; eigrp *
  eigrp *
  clear eigrp *
  debug eigrp *
  show ip eigrp *
  clear ip eigrp *
  debug ip eigrp *
  config t ; router eigrp *
feature: router-isis
  show isis *
  config t ; isis *
  isis *
  clear isis *
  debug isis *
  debug-filter isis *
  config t ; router isis *
feature: router-ospf
  show ospf *
  config t ; ospf *
  ospf *
  clear ospf *
  debug ospf *
  show ip ospf *
  show ospfv3 *
  show ipv6 ospfv3 *
  debug-filter ip ospf *
  debug-filter ospfv3 *
  debug ip ospf *
  debug ospfv3 *
  clear ip ospf *
  clear ip ospfv3 *
  config t ; router ospf *
  config t ; router ospfv3 *
feature: router-rip
  show rip *
  config t ; rip *
  rip *
  clear rip *
  debug rip *
  show ip rip *
  show ipv6 rip *
  overload rip *
  debug-filter rip *
  clear ip rip *
  clear ipv6 rip *
  config t ; router rip *
```

This example shows how to display information for a specific user role feature group:

```
switch(config)# show role feature-group name SecGroup
feature group: SecGroup
feature: aaa
feature: radius
feature: tacacs
```

Related Commands

Command	Description
role feature-group	Configures feature groups for user roles.

Command	Description
rule	Configures rules for user roles.

show role pending

To display the pending user role configuration differences for the Cisco Fabric Services distribution session, use the **show role pending** command.

show role pending

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the user role configuration differences for the Cisco Fabric Services session:

```
switch# show role pending
Role: test-user
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  -------------------------------------------------------------------
  Rule    Perm    Type        Scope           Entity
  -------------------------------------------------------------------
  1       permit  read-write  feature             aaa
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for the user role configuration.

show role pending-diff

To display the differences between the pending user role configuration for the Cisco Fabric Services distribution session and the running configuration, use the **show role pending-diff** command.

show role pending-diff

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the user role configuration differences for the Cisco Fabric Services session:

```
switch# show role pending
+Role: test-user
    +  Description: new role
    +  Vlan policy: permit (default)
    +  Interface policy: permit (default)
    +  Vrf policy: permit (default)
    +  -------------------------------------------------------------------
    +  Rule    Perm    Type        Scope           Entity
    +  -------------------------------------------------------------------
    +  1       permit  read-write  feature             aaa
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for the user role configuration.

show role session

To display the status information for a user role Cisco Fabric Services session, use the **show role session** command.

show role session status

Syntax Description

status	(Optional) Displays the role session status.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the user role configuration differences for the Cisco Fabric Services session:

```
switch# show role session status
Last Action Time Stamp     : Thu Nov 20 12:43:26 2008
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for the user role configuration.

show role status

To display the status for the Cisco Fabric Services distribution for the user role feature, use the **show role status** command.

show role status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example displays the user role configuration differences for the Cisco Fabric Services session:

```
switch# show role status
Distribution: Enabled
Session State: Locked
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for the user role configuration.

show run mka

To display the running configuration of MACsec Key Agreement (MKA), use the **show run mka** command.

show run mka

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the running configuration of MKA:

```
switch# show run mka
!Command: show running-config mka
!Time: Wed Apr 19 05:08:01 2017
version 8.2(0)SK(1)
feature mka
macsec policy p1
   cipher-suite GCM-AES-XPN-128
   key-server-priority 9
   security-policy must-secure
   sak-expiry-time 60
```

Related Commands

Command	Description
cipher suite	Configures the cipher suite for encrypting traffic with MACsec.
conf-offset	Configures the confidentiality offset for MKA encryption.
feature mka	Enables the MKA feature.
key	Creates a key or enters the configuration mode of an existing key.

Command	Description
key chain *keychain-name*	Creates a keychain or enters the configuration mode of an existing keychain.
key-octet-string	Configures the text for a MACsec key.
key-server-priority	Configures the preference for a device to serve as the key server for MKA encryption.
macsec keychain policy	Configures the MACsec keychain policy.
macsec policy	Configures the MACsec policy.
sak-expiry-time *time*	Sets an expiry time for a force SAK rekey.
show key chain	Displays the configuration of the specified keychain.
show macsec policy	Displays all the MACsec policies in the system.

show running-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the running configuration, use the **show running-config aaa** command.

show running-config aaa [all]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

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 display the configured AAA information in the running configuration:

```
switch# show running-config aaa
version 4.0(1)
```

show running-config aclmgr

To display the user-configured access control lists (ACLs) in the running configuration, use the show running-config aclmgr command.

show running-config aclmgr [**all**| **inactive-if-config**]

Syntax Description

all	Displays both the default (CoPP-configured) and user-configured ACLs in the running configuration.
inactive-if-config	Displays the inactive policies in the running configuration.

Command Default

None

Command Modes

Any

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display user-configured ACLs in the running configuration:

```
switch# show running-config aclmgr all
!Command: show running-config aclmgr all
!Time: Wed May 25 08:03:46 2011
version 5.2(1)
ip access-list acl1
ip access-list cisco123-copp-acl-bgp
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ipv6 access-list cisco123-copp-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ip access-list cisco123-copp-acl-cts
  10 permit tcp any any eq 64999
  20 permit tcp any eq 64999 any
ip access-list cisco123-copp-acl-dhcp
  10 permit udp any eq bootpc any
  20 permit udp any neq bootps any eq bootps
ip access-list cisco123-copp-acl-dhcp-relay-response
  10 permit udp any eq bootps any
  20 permit udp any any eq bootpc
ip access-list cisco123-copp-acl-eigrp
```

```
  10 permit eigrp any any
ip access-list cisco123-copp-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list cisco123-copp-acl-glbp
  10 permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list cisco123-copp-acl-hsrp
  10 permit udp any 224.0.0.0/24 eq 1985
ipv6 access-list cisco123-copp-acl-hsrp6
  10 permit udp any ff02::66/128 eq 2029
ip access-list cisco123-copp-acl-icmp
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ipv6 access-list cisco123-copp-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
ipv6 access-list cisco123-copp-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
ip access-list cisco123-copp-acl-igmp
  10 permit igmp any 224.0.0.0/3
mac access-list cisco123-copp-acl-mac-cdp-udld-vtp
  10 permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list cisco123-copp-acl-mac-cfsoe
  10 permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list cisco123-copp-acl-mac-dot1x
  10 permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list cisco123-copp-acl-mac-fabricpath-isis
  10 permit any 0180.c200.0015 0000.0000.0000
  20 permit any 0180.c200.0014 0000.0000.0000
mac access-list cisco123-copp-acl-mac-flow-control
  10 permit any 0180.c200.0001 0000.0000.0000 0x8808
mac access-list cisco123-copp-acl-mac-gold
  10 permit any any 0x3737
mac access-list cisco123-copp-acl-mac-l2pt
  10 permit any 0100.0ccd.cdd0 0000.0000.0000
mac access-list cisco123-copp-acl-mac-lacp
  10 permit any 0180.c200.0002 0000.0000.0000 0x8809
mac access-list cisco123-copp-acl-mac-lldp
  10 permit any 0180.c200.000c 0000.0000.0000 0x88cc
mac access-list cisco123-copp-acl-mac-otv-isis
  10 permit any 0100.0cdf.dfdf 0000.0000.0000
mac access-list cisco123-copp-acl-mac-sdp-srp
  10 permit any 0180.c200.000e 0000.0000.0000 0x3401
mac access-list cisco123-copp-acl-mac-stp
  10 permit any 0100.0ccc.cccd 0000.0000.0000
  20 permit any 0180.c200.0000 0000.0000.0000
mac access-list cisco123-copp-acl-mac-undesirable
  10 permit any any
--More--
```

Related Commands

Command	Description
show running-config copp	Displays the CoPP configuration in the running configuration.
show startup-config aclmgr	Displays the user-configured ACLs in the startup configuration.

Command	Description
show startup-config copp	Displays the CoPP configuration in the startup configuration.

show running-config copp

To display control plane policing configuration information in the running configuration, use the **show running-config copp** command.

show running-config copp [all]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display the configured control plane policing information in the running configuration:

```
switch# show running-config copp
version 4.0(1)
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit exceed
 transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit exceed
 transmit violate drop
```

```
  class copp-system-class-normal
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit exceed
transmit violate drop
```

This example shows how to display the configured and default control plane policing information in the running configuration:

```
switch# show running-config copp all
version 4.0(1)
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit exceed
 transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit exceed
 transmit violate drop
  class copp-system-class-normal
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit exceed
transmit violate drop
```

show running-config cts

To display the Cisco TrustSec configuration in the running configuration, use the **show running-config cts** command.

show running-config cts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any configuration mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

This command requires the Advanced Services license.

Examples

This example shows how to display the Cisco TrustSec configuration in the running configuration:

```
switch# show running-config cts
version 4.0(1)
feature cts
cts role-based enforcement
cts role-based sgt-map 10.10.1.1 10
cts role-based access-list MySGACL
  permit icmp
cts role-based sgt 65535 dgt 65535 access-list MySGACL
cts sxp enable
cts sxp connection peer 10.10.3.3 source 10.10.2.2 password default mode listener
vlan 1
  cts role-based enforcement
vrf context MyVRF
  cts role-based enforcement
```

Related Commands

Command	Description
feature cts	Enables the Cisco TrustSec feature.

show running-config dhcp

To display the Dynamic Host Configuration Protocol (DHCP) snooping configuration in the running configuration and verify other DHCP configurations on a device, use the **show running-config dhcp** command.

show running-config dhcp [all]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.
7.2(0)D1(1)	This command was modified. A sample output for DHCP relay configuration on a Bridge Domain Interface (BDI) was added.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to display the DHCP snooping configuration:

```
switch# show running-config dhcp
version 4.0(1)
feature dhcp
interface Ethernet2/46
  ip verify source dhcp-snooping-vlan
  ip arp inspection trust
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip dhcp snooping vlan 13
ip arp inspection vlan 13
```

This example shows how to verify DHCP configurations on the device. DHCP relay configuration information is also displayed in the example.

```
switch# show running-config dhcp
```

```
version 7.1(0)D1(1)
feature dhcp
service dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn
ipv6 dhcp relay
interface Bdi14
  ip dhcp relay address 10.64.66.242 use-vrf management
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.
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 ip dhcp snooping binding	Displays IP-MAC address bindings, including the static IP source entries.

show running-config dot1x

To display 802.1X configuration information in the running configuration, use the **show running-config dot1x** command.

show running-config dotx1 [all]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the configured 802.1X information in the running configuration:

```
switch# show running-config dot1x
version 4.0(1)
```

show running-config eou

To display the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) configuration information in the running configuration, use the **show running-config eou** command.

show running-config eou [all]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the EAPoUDP feature by using the **feature eou** command before using this command.

This command does not require a license.

Examples

This example shows how to display the configured EAPoUDP information in the running configuration:

```
switch# show running-config eou
version 4.0(1)
```

show running-config ldap

To display Lightweight Directory Access Protocol (LDAP) server information in the running configuration, use the **show running-config ldap** command.

show running-config ldap [all]

Syntax Description

all	(Optional) Displays default LDAP configuration information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display LDAP information in the running configuration:

```
switch# show running-config ldap
```

Related Commands

Command	Description
show ldap-server	Displays LDAP information.

show running-config port-security

To display port-security information in the running configuration, use the **show running-config port-security** command.

show running-config port-security [all]

Syntax Description

all	(Optional) Displays default port-security configuration information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for port-security in the running configuration:

```
switch# show running-port-security
version 4.0(3)
feature port-security
logging level port-security 5
interface Ethernet2/3
  switchport port-security
```

Related Commands

Command	Description
show startup-config port-security	Displays port-security information in the startup configuration.

show running-config radius

To display RADIUS server information in the running configuration, use the **show running-config radius** command.

show running-config radius [all]

Syntax Description

all	(Optional) Displays default RADIUS configuration information.

Command Default

None

Command Modes

Any command mode

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 display information for RADIUS in the running configuration:

```
switch# show running-config radius
```

Related Commands

Command	Description
show radius-server	Displays RADIUS information.

show running-config security

To display a user account, Secure Shell (SSH) server, and Telnet server information in the running configuration, use the **show running-config security** command.

show running-config security [all]

Syntax Description

all	(Optional) Displays the default user account, SSH server, and Telnet server configuration information.

Command Default

None

Command Modes

Any command mode

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 display user account, SSH server, and Telnet server information in the running configuration:

```
switch# show running-config security
version 5.1(1)
username admin password 5 $1$7Jwq/LDM$XF0M/UWeT43DmtjZy8VP91  role network-admin
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network-operator
username user1 password 5 $1$qEclQ5Rx$CAX9fXiAoFPYSvbVzpazj/  role network-operator
telnet server enable
ssh key rsa 1024 force
```

show running-config tacacs+

To display TACACS+ server information in the running configuration, use the **show running-config tacacs+** command.

show running-config tacacs+ [all]

Syntax Description

all	(Optional) Displays default TACACS+ configuration information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you can display TACACS+ information.

This command does not require a license.

Examples

This example shows how to display TACACS+ information in the running configuration:

```
switch# show running-config tacacs+
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ information.

show security system state

To display the status of system related security features, use the **show security system state** command.

show security system state

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display the status of system related security features:

```
switch# show security system state
  XSPACE:
        Non-Executable stack:   Yes
        Non-Executable heap:    Yes
        Non-Writable text:      Yes
  ASLR:
        ASLR enabled:           Yes
        CVE-offset2lib Patch:   Present
        Randomization entropy:  Good
  OSC:
        Version:                1.0.0
  SafeC:
        Version:                3.0.1
```

show software integrity

To display information regarding the runtime integrity feature, use the **show software integrity** command.

show software integrity {**index** *value*| **total**}

Syntax Description

index *value*	Specifies the index value to display hash digest entries. Index 0 indicates starting from the beginning. The index value range is from 0 to 4294967295.
total	Displays the total number of entries in the measurement list.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display the hash digest entries:

```
switch# show software integrity index 0
index pcr template-hash template-name
algorithm:filedata-hash filename-hint
--------------------------------------------------------------------------------------------
1 10 1d8d532d463c9f8c205d0df7787669a85f93e260 ima-ng
sha1:0000000000000000000000000000000000000000 boot_aggregate
2 10 1cb9d1e2795a75857f70d6a23cb77e4843467617 ima-ng
sha256:850c63f1b32f19b2dcde9fa199a83da920c9e377e1e2dc52a6c7fdd045a21475 /etc/r
c.d/rcS.d/S98admin-login
3 10 d07e9ebb0f9b548dd41558a6ec56f62e22b354a0 ima-ng
sha256:941c993b3ffda0e0157442d849304e9a7e96f5f7da551754105023cb2ab8392a /bin/b
ash

switch# show software integrity total
1139
```

show ssh key

To display the Secure Shell (SSH) server key for a virtual device context (VDC), use the **show ssh key** command.

show ssh key

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command is available only when SSH is enabled using the **feature ssh** command.

This command does not require a license.

Examples

This example shows how to display the SSH server key:

```
switch# show ssh key
**************************************
rsa Keys generated:Wed Aug 11 11:45:14 2010
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDypfN6FSHZDbFPWEoz7sgWCamhfoqjqYNoZMvySSb4
056LhWZ75D90KPo+G+XTo7QAyQMpLJSkwKcRkidgD4lwJaDd/Ic/Sl5SJ3i0jyM61Bwvi+8+J3JoIdft
AvgH47GT5BdDD6hM7aUHq+efSQSq8pGyDAR4Cw6UdY9HNAWoTw==
bitcount:1024
fingerprint:
cd:8d:e3:0c:2a:df:58:d3:6e:9c:bd:72:75:3f:2e:45
**************************************
could not retrieve dsa key information
**************************************
```

Related Commands

Command	Description
ssh server key	Configures the SSH server key.

show ssh server

To display the Secure Shell (SSH) server status for a virtual device context (VDC), use the **show ssh server** command.

show ssh server

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the SSH server status:

```
switch# show ssh server
ssh is enabled
version 2 enabled
```

Related Commands

Command	Description
feature ssh	Enables the SSH server.

show startup-config aaa

To display authentication, authorization, and accounting (AAA) configuration information in the startup configuration, use the **show startup-config aaa** command.

show startup-config aaa

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the AAA information in the startup configuration:

```
switch# show startup-config aaa
version 4.0(1)
```

show startup-config aclmgr

To display the user-configured access control lists (ACLs) in the startup configuration, use the show startup-config aclmgr command.

show startup-config aclmgr [all]

Syntax Description

all	Displays both the default (CoPP-configured) and user-configured ACLs in the startup configuration.

Command Default

None

Command Modes

Any

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the user-configured ACLs in the startup configuration:

```
switch(config)# show startup-config aclmgr all
!Command: show startup-config aclmgr all
!Time: Wed May 25 08:04:36 2011
!Startup config saved at: Mon May 23 05:44:16 2011
version 5.2(1)
ip access-list acl1
ip access-list copp-system-p-acl-bgp
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ipv6 access-list copp-system-p-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
ip access-list copp-system-p-acl-cts
  10 permit tcp any any eq 64999
  20 permit tcp any eq 64999 any
ip access-list copp-system-p-acl-dhcp
  10 permit udp any eq bootpc any
  20 permit udp any neq bootps any eq bootps
ip access-list copp-system-p-acl-dhcp-relay-response
  10 permit udp any eq bootps any
  20 permit udp any any eq bootpc
ip access-list copp-system-p-acl-eigrp
  10 permit eigrp any any
ip access-list copp-system-p-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list copp-system-p-acl-glbp
  10 permit udp any eq 3222 224.0.0.0/24 eq 3222
ip access-list copp-system-p-acl-hsrp
  10 permit udp any 224.0.0.0/24 eq 1985
ipv6 access-list copp-system-p-acl-hsrp6
  10 permit udp any ff02::66/128 eq 2029
ip access-list copp-system-p-acl-icmp
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-p-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
ipv6 access-list copp-system-p-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
ip access-list copp-system-p-acl-igmp
  10 permit igmp any 224.0.0.0/3
mac access-list copp-system-p-acl-mac-cdp-udld-vtp
  10 permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-p-acl-mac-cfsoe
  10 permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list copp-system-p-acl-mac-dot1x
  10 permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-p-acl-mac-fabricpath-isis
  10 permit any 0180.c200.0015 0000.0000.0000
  20 permit any 0180.c200.0014 0000.0000.0000
mac access-list copp-system-p-acl-mac-flow-control
--More--
```

Related Commands

Command	Description
show running-config aclmgr	Displays the user-configured ACLs in the running configuration.
show running-config copp	Displays the CoPP configuration in the running configuration.
show startup-config copp	Displays the CoPP configuration in the startup configuration.

show startup-config copp

To display the Control Plane Policing (CoPP) configuration information in the startup configuration, use the **show startup-config copp** command.

show startup-config copp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use this command only in the default virtual device context (VDC).

This command does not require a license.

Examples

This example shows how to display the control plane policing information in the startup configuration:

```
switch# show startup-config copp
version 4.0(1)
class-map type control-plane match-any MyClassMap
  match redirect dhcp-snoop
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
policy-map type control-plane MyPolicyMap
  class MyClassMap
    police cir 0 bps bc 0 bytes conform drop violate drop
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit exceed
 transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit exceed
 transmit violate drop
  class copp-system-class-normal
```

```
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit exceed
transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit exceed
transmit violate drop
policy-map type control-plane x
  class class-default
    police cir 0 bps bc 0 bytes conform drop violate drop
```

show startup-config dhcp

To display the Dynamic Host Configuration Protocol (DHCP) snooping configuration in the startup configuration, use the **show startup-config dhcp** command.

show startup-config dhcp [all]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to display the DHCP snooping configuration in the startup configuration:

```
switch# show startup-config dhcp
version 4.0(1)
feature dhcp
interface Ethernet2/46
  ip verify source dhcp-snooping-vlan
  ip arp inspection trust
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip dhcp snooping vlan 13
ip arp inspection vlan 13
switch#
```

Related Commands

Command	Description
feature dhcp	Enables the DHCP snooping feature on the device.

Command	Description
show running-config dhcp	Shows DHCP snooping configuration in the running configuration.

show startup-config dot1x

To display 802.1X configuration information in the startup configuration, use the **show startup-config dot1x** command.

show startup-config dot1x

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the 802.1X feature by using the **feature dot1x** command before using this command.

This command does not require a license.

Examples

This example shows how to display the 802.1X information in the startup configuration:

```
switch# show startup-config dot1x
version 4.0(1)
```

show startup-config eou

To display the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) configuration information in the startup configuration, use the **show startup-config eou** command.

show startup-config eou

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must enable the EAPoUDP feature by using the **feature eou** command before using this command.

This command does not require a license.

Examples

This example shows how to display the EAPoUDP information in the startup configuration:

```
switch# show startup-config eou
version 4.0(1)
```

show startup-config ldap

To display Lightweight Directory Access Protocol (LDAP) configuration information in the startup configuration, use the **show startup-config ldap** command.

show startup-config ldap

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

You must use the **feature ldap** command before you can display LDAP information.

This command does not require a license.

Examples

This example shows how to display the LDAP information in the startup configuration:

```
switch# show startup-config ldap
!Command: show startup-config ldap
!Time: Wed Feb 17 13:02:31 2010
!Startup config saved at: Wed Feb 17 10:32:23 2010
version 5.0(2)
feature ldap
aaa group server ldap LDAPgroup1
  no ldap-search-map
aaa group server ldap LdapServer1
  no ldap-search-map
```

Related Commands

Command	Description
show ldap-server	Displays LDAP information.

show startup-config port-security

To display port-security information in the startup configuration, use the **show startup-config port-security** command.

show startup-config port-security [all]

Syntax Description

all	(Optional) Displays default port-security configuration information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information for port-security in the startup configuration:

```
switch# show startup-port-security
version 4.0(3)
feature port-security
logging level port-security 5
interface Ethernet2/3
  switchport port-security
```

Related Commands

Command	Description
show running-config port-security	Displays port-security information in the running configuration.

show startup-config radius

To display RADIUS configuration information in the startup configuration, use the **show startup-config radius** command.

show startup-config radius

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the RADIUS information in the startup configuration:

```
switch# show startup-config radius
version 4.0(1)
```

show startup-config security

To display user account, Secure Shell (SSH) server, and Telnet server configuration information in the startup configuration, use the **show startup-config security** command.

show startup-config security

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the user account, SSH server, and Telnet server information in the startup configuration:

```
switch# show startup-config security
version 5.1(1)
username admin password 5 $1$7Jwq/LDM$XF0M/UWeT43DmtjZy8VP91  role network-admin
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network-operator
username user1 password 5 $1$qEclQ5Rx$CAX9fXiAoFPYSvbVzpazj/  role network-operator
telnet server enable
ssh key rsa 1024 force
```

show startup-config tacacs+

To display TACACS+ configuration information in the startup configuration, use the **show startup-config tacacs+** command.

show startup-config tacacs+

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the TACACS+ information in the startup configuration:

```
switch# show startup-config tacacs+
version 4.0(1)
```

show system internal access-list feature bank-chain map

To display the access control list (ACL) ternary content addressable memory (TCAM) bank mapping feature group and combination tables, use the show system internal access-list feature bank-chain map command.

show system internal access-list feature bank-chain map vlan-vlan{**egress**| **ingress**}|**port-vlan**{**egress**| {**interface ingress**| **vlan egress**}} [**module** *module*]

Syntax Description

port-vlan	Specifies the PORT-VLAN mode.
vlan-vlan	Specifies the VLAN-VLAN mode.
ingress	Displays feature class information for ingress modules.
egress	Displays feature class information for egress modules.
module*module*	(Optional) Displays the module.
interface	Displays the mapping output for PORT-VLAN TCAM bank chaining mode for an interface.
vlan	Displays the mapping output for PORT-VLAN TCAM bank chaining mode for a VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.
8.1(1)	The **vlan** and **interface** keywords were introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the feature group and class combination tables for ingress module 2:

```
switch# show system internal access-list feature bank-chain map vlan-vlan ingress module 2
```

```
_________________________________________________________________________
Feature                Rslt Type      T0B0      T0B1      T1B0      T1B1
_________________________________________________________________________
QoS                        Qos         X         X
RACL                       Acl                             X         X
PBR                        Acl                             X         X
VACL                       Acl                             X         X
DHCP                       Acl                             X         X
ARP                        Acl                             X         X
Netflow                    Acl                             X         X
Netflow (SVI)              Acl                             X         X
Netflow Sampler            Acc         X         X
Netflow Sampler (SVI)      Acc         X         X
SPM WCCP                   Acl                             X         X
BFD                        Acl                             X         X
SPM OTV                    Acl                             X         X
ACLMGR ERSPAN (source)     Acl                             X         X
SPM_VINCI_PROXY            Acl                             X         X
SPM_VINCI_ANYCAST          Acl                             X         X
SPM_VINCI_FABRIC_VLAN      Acl                             X         X
SPM ITD                    Acl                             X         X
SPM EVPN ARP               Acl                             X         X
```

The following example displays the mapping output for PORT-VLAN TCAM bank chaining mode for VLAN:

```
# show system internal access-list feature bank-chain map port-vlan vlan ingress
_________________________________________________________________________
Feature                Rslt Type      T0B0      T0B1      T1B0      T1B1
_________________________________________________________________________
QoS                        Qos                             X         X
RACL                       Acl                             X         X
PBR                        Acl                             X         X
VACL                       Acl                             X         X
DHCP                       Acl                             X         X
DHCP_FHS                   Acl                             X         X
DHCP_LDRA                  Acl                             X         X
ARP                        Acl                             X         X
Netflow                    Acl                             X         X
Netflow (SVI)              Acl                             X         X
Netflow Sampler            Acc                             X         X
Netflow Sampler (SVI)      Acc                             X         X
SPM WCCP                   Acl                             X         X
BFD                        Acl                             X         X
SPM OTV                    Acl                             X         X
ACLMGR ERSPAN (source)     Acl                             X         X
SPM_VINCI_PROXY            Acl                             X         X
SPM_VINCI_ANYCAST          Acl                             X         X
SPM_VINCI_FABRIC_VLAN      Acl                             X         X
SPM ITD                    Acl                             X         X
SPM EVPN ARP               Acl                             X         X
UDP RELAY                  Acl                             X         X
SPM_VXLAN_OAM              Acl                             X         X
```

Related Commands

Command	Description
hardware access-list resource feature bank-mapping	Enables ACL TCAM bank mapping for feature groups and classes.

show system internal access-list feature bank-class map

To display the access control list (ACL) ternary content addressable memory (TCAM) bank mapping feature group and class combination tables, use the show system internal access-list feature bank-class map command.

show system internal access-list feature bank-class map {**ingress**| **egress**} [**module** *module*]

Syntax Description

ingress	Displays feature class information for ingress modules.
egress	Displays feature class information for egress modules.
module*module*	(Optional) Displays the module. The range is from 1 to 18.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the feature group and class combination tables for ingress module 4:

```
switch(config)# show system internal access-list feature bank-class map ingress module 4
Feature Class Definition:
0. CLASS_QOS :
QoS,
1. CLASS_INBAND :
Tunnel Decap, SPM LISP, SPM ERSPAN (termination),
2. CLASS_PACL :
PACL, Netflow,
3. CLASS_DHCP :
DHCP, Netflow, ARP, VACL,
4. CLASS_RACL :
RACL, RACL_STAT, Netflow (SVI), ARP,
5. CLASS_VACL :
VACL, VACL_STAT, ARP, FEX, Netflow,
6. CLASS_RV_ACL :
RACL, PBR, BFD, ARP, SPM WCCP, VACL, SPM OTV, FEX, CTS
implicit Tunnel
```

Related Commands

Command	Description
hardware access-list resource feature bank-mapping	Enables ACL TCAM bank mapping for feature groups and classes.

show system internal access-list globals

To display the access control list (ACL) ternary content addressable memory (TCAM) common information along with the bank chaining mode, use the show system internal access-list globals command.

show system internal access-list globals

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the bank chaining mode:

```
switch# show system internal access-list globals
slot  2
=======
        Atomic Update : ENABLED
  Default ACL   : DENY
  Bank Chaining : VLAN-VLAN
  Seq Feat Model : NO_DENY_ACE_SUPPORT
  This pltfm supports seq feat model
  Bank Class Model : DISABLED
  This pltfm supports bank class model
  Fabric path DNL : DISABLED
  Seq Feat Model : NO_DENY_ACE_SUPPORT
  This pltfm supports seq feat model
  L4 proto CAM extend : DISABLED
  This pltfm supports L4 proto CAM extend
  MPLS Topmost As Pipe Mode : DISABLED
  This pltfm supports mpls topmost as pipe mode
  LOU Threshold Value : 5
slot  3
=======
  Atomic Update : ENABLED
  Default ACL   : DENY
  Bank Chaining : PORT-VLAN
  Seq Feat Model : NO_DENY_ACE_SUPPORT
  This pltfm supports seq feat model
  Bank Class Model : DISABLED
  This pltfm supports bank class model
  Fabric path DNL : DISABLED
  Seq Feat Model : NO_DENY_ACE_SUPPORT
  This pltfm supports seq feat model
```

```
L4 proto CAM extend : DISABLED
This pltfm supports L4 proto CAM extend
MPLS Topmost As Pipe Mode : DISABLED
This pltfm supports mpls topmost as pipe mode
LOU Threshold Value : 5
```

Related Commands

Command	Description
hardware access-list resource feature bank-mapping	Enables ACL TCAM bank mapping for feature groups and classes.

show system internal pktmgr internal control sw-rate-limit

To display the inband and outband global rate limit configuration for packets that reach the supervisor module, use the show system internal pktmgr internal control sw-rate-limit command.

show system internal pktmgr internal control sw-rate-limit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the inband and outband global rate limit configuration for packets that reach the supervisor module:

```
switch# show system internal pktmgr internal control sw-rate-limit
inband pps global threshold 12500  outband pps global threshold 15500
switch#
```

Related Commands

Command	Description
rate-limit cpu direction pps action log	Configures rate limits globally on the device for packets that reach the supervisor module.

show system internal udp-relay database

To display the configuration details of the UDP relay feature, use the **show system internal udp-relay database** command.

show system internal udp-relay database

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

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

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the details of the UDP relay feature:

```
switch# show system internal udp-relay database
 UDP Relay enabled : Yes
 Relay enabled on the following UDP Ports:
 ---------------------------------------------------------------
 Sr No.    UDP-Port          Default Port?
 ------    ---------------   ----------------------
   1.        37                  Yes
   2.        42                  Yes
   3.        49                  Yes
   4.        53                  Yes
   5.        69                  Yes
   6.       137                 Yes
   7.       138                 Yes
  -----------------------------------------
 -------------------------------------------
 --------------------------------------------------------
 Object-Group Name      :  iHello
 No. of Relay Addresses :  3
    1 . IP-Addr : 2.6.8.12        Netmask : 255.255.255.255
    2 . IP-Addr : 9.8.7.6         Netmask : 255.255.255.255
    3 . IP-Addr : 2.4.6.8         Netmask : 255.255.0.0
 Associated Interfaces:
 -----------------------------------
    Vlan800             Subnet-broadcast enabled
 ---------------------------------------------------------------
 Object-Group Name      :  iSmart
 No. of Relay Addresses :  1
    1 . IP-Addr : 4.5.6.7         Netmask : 255.255.0.0
 Associated Interfaces:
```

```
-----------------------------------
   Vlan700             Subnet-broadcast disabled
```

Related Commands

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

show tacacs+

To display the TACACS+ Cisco Fabric Services (CFS) distribution status and other details, use the **show tacacs+** command.

show tacacs+ {**distribution status**| **pending [cmds]**| **pending-diff**}

Syntax Description

distribution status	Displays the status of the TACACS+ CFS distribution.
pending	Displays the pending configuration that is not yet applied to the running configuration.
cmds	(Optional) Displays the commands for the pending configuration.
pending-diff	Displays the difference between the active configuration and the pending configuration.

Command Default

None

Command Modes

Any command mode

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 display the TACACS+ CFS status:

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: not yet initiated after enable
last operation: enable
last operation status: success
```

This example shows how to display the TACACS+ merge status:

```
switch# show tacacs+ merge status
Result: Waiting
```

This example shows how to display the pending TACACS+ configuration:

```
switch# show tacacs+ pending
tacacs-server host 10.10.2.2 key 7 qxz12345
```

This example shows how to display the pending TACACS+ configuration commands:

```
switch# show tacacs+ pending cmds
 tacacs-server host 10.10.2.2 key 7 qxz12345 port 49
```

This example shows how to display the differences between the pending TACACS+ configuration and the current TACACS+configuration:

```
switch# show tacacs+ pending-diff
    +tacacs-server host 10.10.2.2
```

show tacacs-server

To display TACACS+ server information, use the **show tacacs-server** command.

show tacacs-server [*hostname*| *ip4-address*| *ipv6-address*] [**directed-request| groups| sorted| statistics**]

Syntax Description

hostname	(Optional) TACACS+ server Domain Name Server (DNS) name. The maximum character size is 256.
ipv4-address	(Optional) TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	(Optional) TACACS+ server IPv6 address in the *X*:*X*:*X*::*X* format.
directed-request	(Optional) Displays the directed request configuration.
groups	(Optional) Displays information about the configured TACACS+ server groups.
sorted	(Optional) Displays sorted-by-name information about the TACACS+ servers.
statistics	(Optional) Displays TACACS+ statistics for the TACACS+ servers.

Command Default

Displays the global TACACS+ server configuration

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

TACACS+ preshared keys are not visible in the **show tacacs-server** command output. Use the **show running-config tacacs+** command to display the TACACS+ preshared keys.

You must use the **feature tacacs+** command before you can display TACACS+ information.

This command does not require a license.

Examples

This example shows how to display information for all TACACS+ servers:

```
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:2
following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
        10.10.1.1:
                available on port:49
```

This example shows how to display information for a specified TACACS+ server:

```
switch# show tacacs-server 10.10.2.2
        10.10.2.2:
                available for authentication on port:1812
                available for accounting on port:1813
                idle time:0
                test user:test
                test password:********
```

This example shows how to display the TACACS+ directed request configuration:

```
switch# show tacacs-server directed-request
enabled
```

This example shows how to display information for TACACS+ server groups:

```
switch# show tacacs-server groups
total number of groups:1
following TACACS+ server groups are configured:
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 0
                vrf is vrf3
```

This example shows how to display information for a specified TACACS+ server group:

```
switch# show tacacs-server groups TacServer
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 0
                vrf is vrf3
```

This example shows how to display sorted information for all TACACS+ servers:

```
switch# show tacacs-server sorted
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:2
following TACACS+ servers are configured:
        10.10.1.1:
                available on port:49
        10.10.2.2:
                available on port:49
```

This example shows how to display statistics for a specified TACACS+ servers:

```
switch# show tacacs-server statistics 10.10.2.2
Server is not monitored
Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
Authorization Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

Related Commands

Command	Description
show running-config tacacs+	Displays the TACACS+ information in the running configuration file.

show telnet server

To display the Telnet server status for a virtual device context (VDC), use the **show telnet server** command.

show telnet server

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display the Telnet server status:

```
switch# show telnet server
telnet service enabled
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

show time-range

To display all time ranges or a specific time range, use the **show time-range** command.

show time-range [*time-range-name*]

Syntax Description

time-range-name	(Optional) Name of a time range, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all time ranges unless you use the *time-range-name* argument to specify a time range.

If you do not specify a time-range name, the device lists time ranges alphabetically by the time-range names.

The output of the **show time-range** command indicates whether a time range is active, which means that the current system time on the device falls within the configured time range.

This command does not require a license.

Examples

This example shows how to use the **show time-range** command without specifying a time-range name on a device that has two time ranges configured, where one of the time ranges is inactive and the other is active:

```
switch(config-time-range)# show time-range
time-range entry: december (inactive)
   10 absolute start 0:00:00 1 December 2009 end 11:59:59 31 December 2009
time-range entry: november (active)
   10 absolute start 0:00:00 1 November 2009 end 23:59:59 30 November 2009
```

Related Commands

Command	Description
time-range	Configures a time range.
permit (IPv4)	Configures a permit rule for an IPv4 ACL.
ipv6 access-list	Configures an IPv6 ACL.

Command	Description
permit (IPv6)	Configures a permit rule for an IPv6 ACL.
permit (MAC)	Configures a permit rule for a MAC ACL.
show ipv6 access-lists	Displays all IPv6 ACLs or a specific IPv6 ACL.
show access-lists	Displays all ACLs or a specific ACL.

show user-account

To display information for the user accounts in a virtual device context (VDC), use the **show user-account** command.

show user-account

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display information for user accounts in the default virtual device context (VDC):

```
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:adminbackup
        this user account has no expiry date
        roles:network-operator
```

This example shows how to display information for user accounts in a nondefault VDC:

```
switch-MyVDC# show user-account
user:admin
        this user account has no expiry date
        roles:vdc-admin
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

show username

To display the public key for the specified user, use the **show username** command.

show username *username* **keypair**

Syntax Description

username	Name of the user. You can enter up to 28 alphanumeric characters.
keypair	Displays the Secure Shell (SSH) user keys.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

For security reasons, this command does not show the private key.

Examples

This example shows how to display the public key for the specified user:

```
switch# show username admin keypair
**************************************
rsa Keys generated:Mon Feb 15 08:10:45 2010
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA0+rIeMgXwv004lt/hwOoyqIKbFGl1tmkFNm/tozuazfL
4dH/asAXZoJePDdiO1ILBGfrQgzyS5u3prXuXfgnWkTu0/4WlD0DF/EPdsd3NNzNbpPFzNDVylPDyDfR
X5SfVICioEirjX9Y59DZP+Nng6rJD7Z/YHVXs/jRNLPBOIs=
bitcount:262144
fingerprint:
a4:a7:b1:d1:43:09:49:6f:7c:f8:60:62:8e:a2:c1:d1
**************************************
could not retrieve dsa key information
**************************************
switch#
```

Related Commands

Command	Description
username username keypair generate	Generates the SSH public and private keys and stores them in the home directory of the Cisco NX-OS device for the specified user.

show users

To display the user session information for a virtual device context (VDC), use the **show users** command.

show users

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

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 display user session information in the default virtual device context (VDC):

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    pts/1        Mar 17 15:18   .          5477 (172.28.254.254)
admin    pts/9        Mar 19 11:19   .         23101 (10.82.234.56)*
```

This example shows how to display information for user accounts in a nondefault VDC:

```
switch-MyVDC# show users
admin     pts/10       Mar 19 12:54   .         30965 (10.82.234.56)*
```

Related Commands

Command	Description
username	Configures user accounts.

show vlan access-list

To display the contents of the IPv4 access control list (ACL), IPv6 ACL, or MAC ACL associated with a specific VLAN access map, use the **show vlan access-list** command.

show vlan access-list *access-list-name*

Syntax Description

access-list-name	Name of the VLAN access map, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

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 use the **show vlan access-list** command to display the contents of the ACL that the VLAN access map named vacl-01 is configured to use:

```
switch# show vlan access-list vacl-01
IP access list ipv4acl
        5 deny ip 10.1.1.1/32 any
        10 permit ip any any
```

Related Commands

Command	Description
vlan access-map	Configures an VLAN access map.
show access-lists	Displays all ACLs or a specific ACL.
show ip access-lists	Displays all IPv4 ACLs or a specific IPv4 ACL.
show ipv6 access-lists	Displays all IPv6 ACLs or a specific IPv6 ACL.
show mac access-lists	Displays all MAC ACLs or a specific MAC ACL.

Command	Description
show vlan access-map	Displays all VLAN access maps or a specific VLAN access map.

show vlan access-map

To display all VLAN access maps or a VLAN access map, use the **show vlan access-map** command.

show vlan access-map *map-name*

Syntax Description

map-name	VLAN access map, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	Command output is sorted alphabetically by the ACL names.
4.0(1)	This command was introduced.

Usage Guidelines

The device shows all VLAN access maps, unless you use the *map-name* argument to specify an access map.

If you do not specify an access-map name, the device lists VLAN access maps alphabetically by access-map name.

For each VLAN access map displayed, the device shows the access-map name, the ACL specified by the **match** command, and the action specified by the **action** command.

Use the **show vlan filter** command to see which VLANs have a VLAN access map applied to them.

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# show vlan access-map
Vlan access-map austin-vlan-map
        match ip: austin-corp-acl
        action: forward
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

show vlan filter

To display information about instances of the **vlan filter** command, including the VLAN access-map and the VLAN IDs affected by the command, use the **show vlan filter** command.

show vlan filter [**access-map** *map-name*| **vlan** *vlan-ID*]

Syntax Description

access-map *map-name*	(Optional) Limits the output to VLANs that the specified access map is applied to.
vlan*vlan-ID*	(Optional) Limits the output to access maps that are applied to the specified VLAN only. Valid VLAN IDs are from 1 to 4096.

Command Default

The device shows all instances of VLAN access maps applied to a VLAN, unless you use the **access-map** keyword and specify an access map, or you use the **vlan** keyword and specify a VLAN ID.

Command Modes

Any command mode

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 display all VLAN access map information on a device that has only one VLAN access map applied (austin-vlan-map) to VLANs 20 through 35 and 42 through 80:

```
switch# show vlan filter
vlan map austin-vlan-map:
        Configured on VLANs:    20-35,42-80
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.

Command	Description
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
vlan access-map	Configures a VLAN access map.
vlan filter	Applies a VLAN access map to one or more VLANs.

T Commands

tacacs+ abort

To discard a TACACS+ Cisco Fabric Services (CFS) distribution session in progress, use the **tacacs+ abort** command.

tacacs+**abort**

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **feature tacacs+** command.

This command does not require a license.

Examples

This example shows how to discard a TACACS+ CFS distribution session in progress:

```
switch# configure terminal
switch(config)# tacacs+ abort
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ distribute	Enables CFS distribution for TACACS+.

tacacs+ commit

To apply the pending configuration pertaining to the TACACS+ Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **tacacs+ commit** command.

tacacs+ commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **feature tacacs+** command.

Before committing the TACACS+ configuration to the fabric, all switches in the fabric must have distribution enabled using the **tacacs+ distribute** command.

CFS does not distribute the TACACS+ server group configurations, periodic TACACS+ server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to apply a TACACS+ configuration to the switches in the fabric.

```
switch# configure terminal
switch(config)# tacacs+ commit
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ distribute	Enables CFS distribution for TACACS+.

tacacs+ distribute

To enable Cisco Fabric Services (CFS) distribution for TACACS+, use the **tacacs+ distribute** command. To disable this feature, use the **no** form of the command.

tacacs+ **distribute**

no tacacs+ **distribute**

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **feature tacacs+** command.

CFS does not distribute the TACACS+ server group configurations, periodic TACACS+ server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to enable TACACS+ fabric distribution:

```
switch# configure terminal
switch(config)# tacacs+ distribute
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs+	Displays TACACS+ CFS distribution status and other details.

tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

tacacs-server deadtime minutes

no tacacs-server deadtime minutes

Syntax Description

time	Time interval in minutes. The range is from 1 to 1440.

Command Default

0 minutes

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

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 dead-time interval and enable periodic monitoring:

```
switch# configure terminal
switch(config)# tacacs
-server deadtime 10
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
switch# configure terminal
switch(config)# no tacacs
-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a dead-time interval for monitoring a nonresponsive TACACS+ server.
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the**tacacs-server directed request** command. To revert to the default, use the **no** form of this command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Sends the authentication request to the configured TACACS+ server groups

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

The user can specify the *username@vrfname* :*hostname* during login, where vrfname is the virtual routing and forwarding (VRF) name to use and hostname is the name of a configured TACACS+ server. The username is sent to the server name for authentication.

Note If you enable the directed-request option, the Cisco NX-OS device uses only the RADIUS method for authentication and not the default local method.

This command does not require a license.

Examples

This example shows how to allow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch# configure terminal
switch(config)# tacacs
-server
directed-request
```

This example shows how to disallow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch# configure terminal
switch(config)# no tacacs
-server
directed-request
```

Related Commands

Command	Description
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.
feature tacacs+	Enables TACACS+.

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command. To revert to the default setting, use the **no** form of this command.

tacacs-server host {*hostname*| *ipv4-address*| *ipv6-address*} [**key** [**0**| **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time time**| **password password**| **username name**}] [**timeout** *seconds*] **[single-connection]**

no tacacs-server host {*hostname*| *ipv4-address*| *ipv6-address*} [**key** [**0**| **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time time**| **password password**| **username name**}] [**timeout** *seconds*] **[single-connection]**

Syntax Description

hostname	TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	TACACS+ server IPv6 address in the *X*:*X*:*X*:*X* format.
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(Optional) Configures a preshared key specified in cleartext (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.
port *port-number*	(Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.

password *password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username *name*	Specifies a username in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters.
timeout *seconds*	(Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.
single-connection	(Optional) Configures a single connection for the TACACS+ server.

Command Default

Idle time: disabled

Server monitoring: disabled

Timeout: 1 second.

Test username: test

Test password: test

Command Modes

Global configuration

Command History

Release	Modification
6.2(2)	The single-connection keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

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

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

This command does not require a license.

Examples

This example shows how to configure TACACS+ server host parameters:

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

tacacs-server key

To configure a global TACACS+ shared secret key, use the**tacacs-server key** command. To removed a configured shared secret, use the **no** form of this command.

tacacs-server key [**0**| **6**| **7**] *shared-secret*

no tacacs-server key [**0**| **6**| **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default.
6	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must configure the TACACS+ preshared key to authenticate the device to the TACACS+ server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the device. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

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

This command does not require a license.

Examples

The following example shows how to configure TACACS+ server shared keys:

```
switch# configure terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

tacacs-server test

To monitor the availability of all TACACS+ servers without having to configure the test parameters for each server individually, use the**tacacs-server test** command. To disable this configuration, use the **no** form of this command.

tacacs-server test {**idle-time time**| **password password**| **username name**}

no tacacs-server test {**idle-time time**| **password password**| **username name**}

Syntax Description

idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes. **Note** When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.
password *password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username *name*	Specifies a username in the test packets. The name is alphanumeric, not case sensitive, and has a maximum of 32 characters. **Note** To protect network security, we recommend that you use a username that is not the same as an existing username in the TACACS+ database.

Command Default

Server monitoring: Disabled

Idle time: 0 minutes

Test username: test

Test password: test

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable TACACS+ authentication.

Any servers for which test parameters are not configured are monitored using the global level parameters.

Test parameters that are configured for individual servers take precedence over global test parameters.

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

This command does not require a license.

Examples

This example shows how to configure the parameters for global TACACS+ server monitoring:

```
switch# configure terminal
switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the**tacacs-server timeout** command. To revert to the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Seconds between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Command Default

1 second

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	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 TACACS+ server timeout value:

```
switch# configure terminal
switch(config)# tacacs-server timeout 3
```

This example shows how to revert to the default TACACS+ server timeout value:

```
switch# configure terminal
switch(config)# no tacacs-server timeout 3
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

telnet

To create a Telnet session using IPv4 on the Cisco NX-OS device, use the **telnet** command.

telnet {*ipv4-address*| *hostname*} [*port-number*] [**vrf** *vrf-name*]

Syntax Description

ipv4-address	IPv4 address of the remote device.
hostname	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf*vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive.

Command Default

Port 23

Default VRF

Command Modes

Any command mode

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Telnet server using the **feature telnet** command.

To create a Telnet session with IPv6 addressing, use the **telnet6** command.

The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

This command does not require a license.

Examples

This example shows how to start a Telnet session using an IPv4 address:

```
switch# telnet 10.10.1.1 vrf management
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
telnet6	Creates a Telnet session using IPv6 addressing.
feature telnet	Enables the Telnet server.

telnet server enable

To enable the Telnet server for a virtual device context (VDC), use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command.

telnet server enable

no telnet server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
4.1(2)	This command was deprecated and replaced with the **feature telnet** command.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the Telnet server:

```
switch# configure terminal
switch(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
switch# configure terminal
switch(config)# no telnet server enable
XML interface to system may become unavailable since ssh is disabled
```

Related Commands

Command	Description
show telnet server	Displays the SSH server key information.

telnet6

To create a Telnet session using IPv6 on the Cisco NX-OS device, use the **telnet6** command.

telnet6 {*ipv6-address*| *hostname*} [*port-number*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	IPv6 address of the remote device.
hostname	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf*vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive.

Command Default

Port 23

Default VRF

Command Modes

Any command mode

Command History

Release	Modification
4.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Telnet server using the **feature telnet** command.

To create a Telnet session with IPv4 addressing, use the **telnet** command.

The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

This command does not require a license.

Examples

This example shows how to start a Telnet session using an IPv6 address:

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
telnet	Creates a Telnet session using IPv4 addressing.
feature telnet	Enables the Telnet server.

terminal verify-only

To enable command authorization verification on the command-line interface (CLI), use the **terminal verify-only** command. To disable this feature, use the **no** form of this command.

terminal verify-only [**username** *username*]

terminal no verify-only [**username** *username*]

Syntax Description

username *username*	(Optional) Specifies the username for which to verify command authorization.

Command Default

Disabled

The default for the **username** keyword is the current user session.

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

When you enable command authorization verification, the CLI indicates if the command is successfully authorized for the user but does not execute the command.

The command authorization verification uses the methods configured in the **aaa authorization commands default** command and the **aaa authorization config-commands default** command.

This command does not require a license.

Examples

This example shows how to enable command authorization verification:

```
switch# terminal verify-only
```

This example shows how to disable command authorization verification:

```
switch# terminal no verify-only
```

Related Commands

Command	Description
aaa authorization commands default	Configures authorization for EXEC commands.

Command	Description
aaa authorization config-commands default	Configures authorization for configuration commands.

test aaa authorization command-type

To test the TACACS+ command authorization for a username, use the **test aaa authorization command-type** command.

test aaa authorization command-type {**commands**| **config-commands**} **user** *username* **command** *command-string*

Syntax Description

commands	Tests EXEC commands.
config-commands	Tests configuration commands.
user *username*	Specifies the user name for TACACS+ command authorization testing.
command *command-string*	Specifies the command for authorization testing. Put double quotes around the *command-string* argument if the command contains spaces.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

To use the **test aaa authorization command-type** command, you must enable the TACACS+ feature using the **feature tacacs+** command.

You must configure a TACACS+ group on the Cisco NX-OS device using the **aaa server group** command before you can test the command authorization.

This command does not require a license.

Examples

This example shows how to test the TACACS+ command authorization for a username:

```
switch# test aaa authorization command-type commands user testuser command “configure terminal”
```

Related Commands

Command	Description
aaa authorization commands default	Configures authorization for EXEC commands.
aaa authorization config-commands default	Configures authorization for configuration commands.
aaa group server	Configures AAA server groups.

time-range

To configure a time range, use the**time-range** command. To remove a time range, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description

time-range-name	Name of the time range, which can be up to 64 alphanumeric, case-sensitive characters.

Command Default

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.

You can use a time range in **permit** and **deny** commands for IPv4 and IPv6 ACLs.

Examples

This example shows how to use the **time-range** command and enter time range configuration mode:

```
switch# configure terminal
switch(config)# time-range workweek-vpn-access
switch(config-time-range)#
```

Related Commands

Command	Description
absolute	Specifies a time range that has a specific start date and time.
deny (IPv4)	Configures an IPv4 deny rule.
deny (IPv6)	Configures an IPv6 deny rule.
periodic	Specifies a time range that is active one or more times per week.

Command	Description
permit (IPv4)	Configures an IPv4 permit rule.
permit (IPv6)	Configures an IPv6 permit rule.

trustedCert

To configure the attribute name, search filter, and base-DN for the trusted certificate search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **trustedCert** command. To disable this configuration, use the **no** form of this command.

trustedCert attribute-name attribute-name search-filter filter base-DN base-DN-name

no trustedCert

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the trusted certificate search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# trustedCert attribute-name cACertificate search-filter
(&(objectClass=certificationAuthority)) base-DN CN=NTAuthCertificates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=mdsldaptestlab,DC=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

U Commands

user-certdn-match

To configure the attribute name, search filter, and base-DN for the certificate DN match search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-certdn-match** command. To disable this configuration, use the **no** form of this command.

user-certdn-match attribute-name attribute-name search-filter filter base-DN base-DN-name

no user-certdn-match

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the certificate DN match search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-certdn-match attribute-name certificateDN search-filter
 (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

username

To create and configure a user account in a virtual device context (VDC), use the **username** command. To remove a user account, use the **no** form of this command.

username *user-id* [**expire** *date*] [**password** [**0**| **5**] *password*] [**role** *role-name*]

username *user-id* [**sshkey** {*key*| **file** *filename*}]

username *user-id* [**keypair generate** {**rsa** [**bits [force]**]| **dsa [force]**}]

username *user-id* [**keypair** {**export**| **import**} {**bootflash**:**filename**| **volatile**:**filename**} {**rsa**| **dsa**} **[force]**]

username *user-id* [**priv-lvl** *n*] [**expire** *date*] [**password** [**0**| **5**] *password*]

username *user-id* [**ssh-cert-dn** *dn-name*{**rsa**}]

no username *user-id*

Syntax Description

user-id	User identifier for the user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. For more information, see the usage guidelines section below. **Note** The Cisco NX-OS software allows these special characters in the *user-id* argument text string: (_ . + = \ -).
expire *date*	(Optional) Specifies the expire date for the user account. The format for the *date* argument is YYYY-MM-DD.
password	(Optional) Specifies a password for the account. The default is no password.
0	(Optional) Specifies that the password is in clear text. Clear text passwords are encrypted before they are saved to the running configuration.
5	(Optional) Specifies that the password is in encrypted format. Encrypted passwords are not changed before they are saved to the running configuration.
password	Password string. The password is alphanumeric, case sensitive, and has a maximum of 64 characters. **Note** All printable ASCII characters are supported in the password string if they are enclosed in quotation marks.
role *role-name*	(Optional) Specifies the user role. The *role-name* argument is case sensitive.

sshkey	(Optional) Specifies an SSH key for the user account.
key	SSH key string.
file *filename*	Specifies the name of a file that contains the SSH key string.
keypair	Generates SSH user keys.
generate	Generates SSH key-pairs.
bits	Number of bits used to generate the key. The range is from 1024 to 2048, and the default value is 1024.
force	Forces the generation of keys even if previous ones are present.
rsa	Generates Rivest, Shamir, and Adelman (RSA) keys.
export	Exports key-pairs to the bootflash or volatile directory.
import	Imports key-pairs from the bootflash or volatile directory.
ssh-cert-dn	Specifies an SSH X.509 certificate distinguished name RSA algorithm to use for authentication for an existing user account.
dn-name	Specifies the distinguished name, which can be up to 512 characters and must follow the Open SSL format.
bootflash:*filename*	Specifies the bootflash filename.
volatile:*filename*	Specifies the remote filename.
priv-lvl *n*	Specifies the privilege level to which the user is assigned. The range is from 0 to 15.

Command Default

Unless specified, usernames have no expire date, password, or SSH key.

In the default VDC, the default role is network-operator if the creating user has the network-admin role, or the default role is vdc-operator if the creating user has the vdc-admin role.

In nondefault VDCs, the default user role is vdc-operator.

You cannot delete the default admin user role. Also, you cannot change the expire date or remove the network-admin role for the default admin user role.

To specify privilege levels, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command. There is no default privilege level.

This command does not require a license.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	Added the **ssh-cert-dn** keyword option.
5.1(1)	Removed support for RSA keys less than 1024 bits.
5.0(2)	Added the **keypair** keyword option.
5.0(2)	Added the **priv-lvl** keyword option.
4.1(2)	Added the **sshkey** keyword option.
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software creates two default user accounts in the VDC: admin and adminbackup. The nondefault VDCs have one default user account: admin. You cannot remove a default user account.

User accounts are local to the VDCs. You can create user accounts with the same user identifiers in different VDCs.

Caution The Cisco NX-OS software does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

The Cisco NX-OS software accepts only strong passwords when you have password-strength checking enabled using the **password strength-check** command. The characteristics of a strong password include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Caution If you do not specify a password for the user account, the user might not be able to log in to the account.

To use this command, you must enable the cumulative privilege of roles using the **feature privilege** command.

A passphrase is required when you export or import the key-pair. The passphrase encrypts the exported private key for the user and decrypts it during import.

This command does not require a license.

Examples

This example shows how to create a user account with a password and a user role:

```
switch# configure t
switch(config)# username user1 password Ci5co321 role vdc-admin
```

This example shows how to configure the SSH key for a user account:

```
switch# configure t
switch(config)# username user1 sshkey file bootflash:key_file
```

This example shows how to generate the SSH public and private keys and store them in the home directory of the Cisco NX-OS device for the user:

```
switch# configure t
switch(config)# username user1 keypair generate rsa
generating rsa key(2048 bits)......
generated rsa key
```

This example shows how to export the public and private keys from the home directory of the Cisco NX-OS device to the bootflash directory:

```
switch# configure t
switch(config)# username user1 keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
951 Jul 09 11:13:59 2009 key_rsa
221 Jul 09 11:14:00 2009 key_rsa.pub
.
.
```

The private key is exported as the file that you specify, and the public key is exported with the same filename followed by a .pub extension.

This example shows how to import the exported public and private keys from the bootflash directory to the home directory of the Cisco NX-OS device:

```
switch# configure t
switch(config)# username user1 keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username user1 keypair
**************************************
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************
could not retrieve dsa key information
```

```
*************************************
switch(config)#
```

The private key is imported as the file that you specify, and the public key is imported with the same filename followed by a .pub extension.

This example shows how to assign privilege level 15 to the user:

```
switch# configure t
switch(config)# feature privilege
switch(config)# enable secret 5 def456 priv-lvl 15
switch(config)# username user2 priv-lvl 15
```

This example shows how to configure X.509v3 certificate-based SSH authentication.

```
switch# configure terminal
switch(config)# username jsmith password 4Ty18Rnt
switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
rsa
switch(config)# crypto ca trustpoint tp1
switch(config-trustpoint)# crypto ca authenticate tp1
switch(config-trustpoint)# crypto ca crl request tp1 bootflash:crl1.crl
switch(config-trustpoint)# exit
switch(config)# exit
```

Related Commands

Command	Description
enable *level*	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
password strength-check	Checks the password security strength.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
show user-account	Displays the user account configuration.
show username	Displays the public key for the specified user.

userprofile

To configure the attribute name, search filter, and base-DN for the user profile search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **userprofile** command. To disable this configuration, use the **no** form of this command.

userprofile attribute-name attribute-name search-filter filter base-DN base-DN-name

no userprofile

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the user profile search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# userprofile attribute-name description search-filter
(&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

user-pubkey-match

To configure the attribute name, search filter, and base-DN for the public key match search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-pubkey-match** command. To disable this configuration, use the **no** form of this command.

user-pubkey-match attribute-name attribute-name search-filter filter base-DN base-DN-name

no user-pubkey-match

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the public key match search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-pubkey-match attribute-name sshPublicKey search-filter
 (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

user-switch-bind

To configure the attribute name, search filter, and base-DN for the user-switchgroup search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-switch-bind** command. To disable this configuration, use the **no** form of this command.

user-switch-bind attribute-name attribute-name search-filter filter base-DN base-DN-name

no user-switch-bind

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the user-switchgroup search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-switch-bind attribute-name memberuid search-filter
(&(objectClass=posixGroup)(cn=dcgroup)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

use-vrf

To specify a virtual routing and forwarding instance (VRF) name for a RADIUS, TACACS+, or LDAP server group, use the**use-vrf** command. To remove the VRF name, use the **no** form of this command.

use-vrf *vrf-name*

no use-vrf *vrf-name*

Syntax Description

vrf-name	VRF name. The name is case sensitive.

Command Default

None

Command Modes

RADlUS server group configurationTACACS+ server group configurationLDAP server group configuration

Command History

Release	Modification
5.0(2)	Added support for LDAP server groups.
4.0(1)	This command was introduced.

Usage Guidelines

You can configure only one VRF instance for a server group.

Use the **aaa group server radius** command to enter RADIUS server group configuration mode, the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode, or the **aaa group server ldap** command to enter LDAP server group configuration mode.

If the server is not found, use the **radius-server host** command, the **tacacs-server host** command, or the **ldap-server host** command to configure the server.

Note You must use the **feature tacacs+** command before you configure TACACS+ or the **feature ldap** command before you configure LDAP.

This command does not require a license.

Examples

This example shows how to specify a VRF name for a RADIUS server group:

```
switch# configure t
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf vrf1
```

This example shows how to specify a VRF name for a TACACS+ server group:

```
switch# configure t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf vrf2
```

This example shows how to remove the VRF name from a TACACS+ server group:

```
switch# configure t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf vrf2
```

This example shows how to specify a VRF name for an LDAP server group:

```
switch# configure t
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-tacacs+)# use-vrf vrf3
```

This example shows how to remove the VRF name from an LDAP server group:

```
switch# configure t
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-tacacs+)# no use-vrf vrf3
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures a RADIUS server.
show ldap-server groups	Displays LDAP server information.
show radius-server groups	Displays RADIUS server information.
show tacacs-server groups	Displays TACACS+ server information.
feature ldap	Enables LDAP.
feature tacacs+	Enables TACACS+.
ldap-server host	Configures an LDAP server.
tacacs-server host	Configures a TACACS+ server.
vrf	Configures a VRF instance.

V Commands

vlan access-map

To create a new VLAN access-map entry or to configure an existing VLAN access-map entry, use the **vlan access-map** command. To remove a VLAN access-map entry, use the **no** form of this command.

vlan access-map *map-name* [*sequence-number*]

no vlan access-map *map-name* [*sequence-number*]

Syntax Description

sequence-number	(Optional) Sequence number of the VLAN access-map entry that you are creating or editing. A sequence number can be any integer between 1 and 4294967295. By default, the first entry in a VLAN access map has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the VLAN access map and assigns a sequence number that is 10 greater than the sequence number of the preceding entry. When you use the **no** form of the command, use the *sequence-number* argument to specify an entry that you want to remove. Omit the *sequence-number* argument if you want to remove the entire VLAN access map.
map-name	Name of the VLAN access map that you want to create or configure. The *map-name* argument can be up to 64 alphanumeric, case-sensitive characters.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Each VLAN access-map entry can include one **action** command and one or more **match** command.

Use the **statistics per-entry** command to configure the device to record statistics for a VLAN access-map entry.

This command does not require a license.

Examples

This example shows how to create a VLAN access map named vlan-map-01, add two entries that each have two **match** commands and one **action** command, and enable statistics for the packets matched by the second entry:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# match mac address mac-acl-00f
switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-320
switch(config-access-map)# match mac address mac-acl-00e
switch(config-access-map)# action drop
switch(config-access-map)# statistics per-entry
switch(config-access-map)# show vlan access-map
Vlan access-map vlan-map-01 10
        match ip: ip-acl-01
        match mac: mac-acl-00f
        action: forward
Vlan access-map vlan-map-01 20
        match ip: ip-acl-320
        match mac: mac-acl-00e
        action: drop
        statistics per-entry
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
vlan filter	Applies a VLAN access map to one or more VLANs.

vlan filter

To apply a VLAN access map to one or more VLANs, use the **vlan filter** command. To unapply a VLAN access map, use the **no** form of this command.

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* **vlan-list** *VLAN-list*

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure.
vlan-list *VLAN-list*	Specifies the ID of one or more VLANs that the VLAN access map filters. Valid VLAN IDs are from 1 to 4096. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, use 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, use 20,70-100,142. **Note** When you use the **no** form of this command, the *VLAN-list* argument is optional. If you omit this argument, the device removes the access map from all VLANs where the access map is applied.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can apply a VLAN access map to one or more VLANs.

You can apply only one VLAN access map to a VLAN.

The **no** form of this command enables you to unapply a VLAN access map from all or part of the VLAN list that you specified when you applied the access map. To unapply an access map from all VLANs where it is applied, you can omit the *VLAN-list* argument. To unapply an access map from a subset of the VLANs where it is currently applied, use the *VLAN-list* argument to specify the VLANs where the access map should be removed.

This command does not require a license.

Examples

This example shows how to apply a VLAN access map named vlan-map-01 to VLANs 20 through 45:

```
switch# configure t
switch(config)# vlan filter vlan-map-01 20-45
```

This example show how to use the **no** form of the command to unapply the VLAN access map named vlan-map-01 from VLANs 30 through 32, which leaves the access map applied to VLANs 20 through 29 and 33 through 45:

```
switch# show vlan filter
vlan map vlan-map-01:
        Configured on VLANs:    20-45
switch(config)# no
 vlan filter vlan-map-01 30-32
switch# show vlan filter
vlan map vlan-map-01:
        Configured on VLANs:    20-29,33-45
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.

vlan policy deny

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

vlan policy deny

no vlan policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All VLANs

Command Modes

User role configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

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

```
switch# configure t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

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

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

Related Commands

Command	Description
permit vlan	Allows a VLAN in a user role VLAN policy.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

vrf policy deny

To enter virtual forwarding and routing instance (VRF) policy configuration mode for a user role, use the**vrf policy deny** command. To revert to the default VRF policy for a user role, use the **no** form of this command.

vrf policy deny

no vrf policy deny

Syntax Description

This command has no arguments or keywords.

Command Default

All VRFs

Command Modes

User role configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

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

```
switch# configure t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

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

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

Related Commands

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