R to S Commands

This chapter describes the Cisco NX-OS Security commands that begin with R to S.

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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*]]

no 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*]]

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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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 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.

Defaults

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.

Defaults

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.

Defaults

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:

```
witch# 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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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.
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.

Defaults

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.

Defaults

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.

Defaults

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.

Defaults

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.
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.*

Defaults

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.

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.

Defaults

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.

Defaults

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.

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.

Defaults

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** | **gcm-encrypt-256** | **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.
gcm-encrypt-256	Specifies 256-bit 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.

Defaults

gcm-encrypt

Command Modes

Cisco TrustSec manual configuration

Command History

Release	Modification
7.3(0)DX(1)	This command was modified. The **gcm-encrypt-256** keyword was added.
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 will be supported based on capability of the line card. Only M3 is currently capable and hence this will not be supported older generation line cards such as M1, M2, F1, F2, and F3. 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 gcm-encrypt-256
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.

Defaults

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.

Defaults

None

Command Modes

RADIUS server group configuration
TACACS+ server group configuration
LDAP 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.

Defaults

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.
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.

Defaults

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.
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.

Defaults

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.

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.

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).

Defaults

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.

Defaults

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**.

Defaults

The default is the global source interface.

Command Modes

RADIUS configuration
TACACS+ 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.
ip tacacs source-interface	Configures the global source interface for the TACACS+ groups configured on the Cisco NX-OS device.

Command	Description
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.

Defaults

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.

Defaults

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.

Defaults

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# config t
switch(config)# ssh login-attempts 5
```

This example shows how to disable the SSH login attempt configuration:

```
switch# config t
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.

Defaults

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# config t
switch(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
switch# config t
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.

Defaults

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.
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.

Defaults

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.

Defaults

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.

Defaults

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 time

To configure the aging time for dynamically learned, secure MAC addresses, use the **switchport port-security aging time** command. To return to the default aging time of 1440 minutes, use the **no** form of this command.

switchport port-security aging time *minutes*

no switchport port-security aging time *minutes*

Syntax Description

minutes	Length of time that a dynamically learned, secure MAC address must age before the device drops the address. Valid values are from 1 to 1440.

Defaults

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 aging time is 1440 minutes.

You must enable port security by using the **feature port-security** command before you can use the **switchport port-security aging time** 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 an aging time of 120 minutes on the Ethernet 2/1 interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security aging time 120
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.

Command	Description
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.

Defaults

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.

Defaults

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.

Defaults

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.
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.

Command	Description
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.

Defaults

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.

Defaults

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.

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.

Defaults

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.