



## S Commands

---

This chapter describes the Cisco NX-OS security commands that begin with S, except for **show** [Chapter 2, “Show Commands.”](#)

### 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		
	<b>gcm-encrypt</b>	Specifies Galois/Counter Mode (GCM) encryption and authentication mode.
	<b>gmac</b>	Specifies GCM authentication mode.
	<b>no-encap</b>	Specifies no encapsulation and no security group tag (SGT) insertion.
	<b>none</b>	Specifies the encapsulation of the SGT without authentication or encryption.

Defaults	
	<b>gcm-encrypt</b>

Command Modes	
	Cisco TrustSec 802.1X configuration

Supported User Roles	
	network-admin vdc-admin

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

**Usage Guidelines**

To use this command, you must enable the 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# config t
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
```

```
switch# config t
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
```

---

<b>cts dot1x</b>	Enters Cisco TrustSec 802.1X configuration mode for an interface.
	Enables the Cisco TrustSec feature.
	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 sap pmk` form of this command.

```
sap pmk [key key [no-auth] [no-enc] [no-enc-auth] [no-enc-encap] [no-enc-encap-auth] [no-enc-encap-auth-encap] ]
```

## Syntax Description

<i>key</i>	Key value. This is a hexadecimal string with an even number of characters. The maximum length is 32 characters.
<code>no-auth</code>	Specifies that the peer device does not support Cisco TrustSec 802.1X authentication or authorization but does support SAP data path encryption and authentication.
<code>no-enc</code>	(Optional) Specifies the SAP operation mode.
<code>no-enc-auth</code>	Specifies Galois/Counter Mode (GCM) encryption and authentication mode.
<code>no-enc-encap</code>	Specifies GCM authentication mode.
<code>no-enc-encap-auth</code>	Specifies no encapsulation and no security group tag (SGT) insertion.
<code>no-enc-encap-auth-encap</code>	Specifies the encapsulation of the SGT without authentication or encryption.

## Defaults

## Command Modes

Cisco TrustSec manual configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(3)	The <code>no-enc-encap-auth-encap</code> keyword was added.
4.0(1)	This command was introduced.

## Usage Guidelines

To use this command, you must enable the Cisco TrustSec feature using the `trustsec enable` command. After using this command, you must enable and disable the interface using the `trustsec enable` / `trustsec disable` 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#
switch(config)#
switch(config-if)#
switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

```
switch# config t
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

# send-lifetime

*start-time*      *duration-value* | **infinite** | *end-time*

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

## infinite

4.0(1)	This command was introduced.
--------	------------------------------

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            and            arguments both require time and date components, in the following format:

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

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

---

This 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:

```
configure terminal
  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)#
```

---

---

---

---

---

---

---

---

# server

To add a server to a RADIUS or TACACS+ 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* }

<i>ipv4-address</i>	<i>A.B.C.D</i>
<i>ipv6-address</i>	<i>X:X:X::X</i>
<i>hostname</i>	

None

RADIUS server group configuration  
TACACS+ server group configuration

network-admin  
vdc-admin

Release	Modification

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 or the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.



Note

feature tacacs+

## Examples

```
switch#
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
```

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 10.10.1.1
```

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
```

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 10.10.2.2
```

## Related Commands

Command	Description

# service dhcp

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

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** Global configuration

**Supported User Roles** network-admin  
vdc-admin

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

**Usage Guidelines** This command does not require a license.

**Examples** This example shows how to globally enable DHCP snooping:

```
switch# configure terminal
switch(config)# service dhcp
switch(config)#
```

Related Commands	Command	Description
	<code>service dhcp</code>	Enables the DHCP snooping feature on the device.
	<code>ip dhcp server address</code>	Configures an IP address of a DHCP server on an interface.
	<code>ip dhcp snooping</code>	Enables the insertion and removal of option-82 information from DHCP packets.
	<code>ip dhcp snooping global</code>	Globally enables DHCP snooping on the device.
	<code>show ip dhcp snooping</code>	Displays general information about DHCP snooping.
	<code>show ip dhcp snooping configuration</code>	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 service-policy input` form of this command.

---

## Syntax Description

---



---

## Defaults

None

---

## Command Modes

Control plane configuration

---

## Supported User Roles

network-admin  
vdc-admin

---

## Command History

Release	Modification

---



---

## Usage Guidelines

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

You can assign only one control plane 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# config t
switch(config)# control-plane
switch(config-cp)# service-policy input PolicyMapA

switch# config t
switch(config)# control-plane
switch(config-cp)# no service-policy input PolicyMapA

```

Related Commands	Command	Description

## set cos

To set the IEEE 802.1Q class of service (CoS) value for a control plane policy map, use the command. To revert to the default, use the form of this command.

```
[ ]
```

```
[ ]
```

---

(Optional) Specifies inner 802.1Q in a Q-in-Q environment.

---

Numerical value of CoS in the control plane policy map. The range is from 0 to 7.

---



---

0

---

Policy map class configuration

---

network-admin  
vdc-admin

---

4.0(1)

---

This command was introduced.

---



---

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

This command does not require a license.

---

This example shows how to configure the CoS value for a control plane policy map:

```
switch# config t
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# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set cos 4
```

---

**class (policy map)**

---

**policy-map type  
control-plane**

---

**show policy-map type  
control-plane**

---

# set dscp (policy map class)

```

set dscp tunnel          set dscp          no
                        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      af11 af12 af13 af21 af22 af23 af31 af32 af33 af41
                        af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 ef default
    
```

**Syntax Description**

tunnel
af11
af12
af13
af21
af22
af23
af31
af32
af33
af41
af42
af43
cs1
cs2
cs3
cs4
cs5
cs6
cs7
ef
default

**Defaults**

default

**Command Modes**

---

**SupportedUserRoles**


---

**Command History**

Release	Modification

---

**Usage Guidelines**


---

**Examples**

```
switch#
switch(config)#
switch(config-pmap)#
switch(config-pmap-c)#
```

```
switch#
switch(config)#
switch(config-pmap)#
switch(config-pmap-c)#
```

---

**Related Commands**

Command	Description
<b>class (policy map)</b>	
<b>policy-map type control-plane</b>	
<b>show policy-map type control-plane</b>	

# set precedence (policy map class)

```


```

precedence                               no                               set
set precedence tunnel                    critical flash flash-override immediate internet
  network priority routine
no set precedence tunnel                  critical flash flash-override immediate internet
  network priority routine

```


```

## Syntax Description

tunnel

critical

flash

flash-override

immediate

internet

network

priority

routine

## Defaults

routine

## Command Modes

## Supported User Roles

## Command History

Release

Modification

## Usage Guidelines

---

**Examples**

```
switch#  
switch(config)#  
switch(config-pmap)#  
switch(config-pmap-c)#
```

```
switch#  
switch(config)#  
switch(config-pmap)#  
switch(config-pmap-c)#
```

---

**Related Commands**

Command	Description
<b>class (policy map)</b>	
<b>policy-map type control-plane</b>	
<b>show policy-map type control-plane</b>	

# ssh

ssh

ssh @ vrf vrf-name

## Syntax Description

---

*username*

---

*ipv4-address*

---

*hostname*

---

**vrf** *vrf-name*

---

## Defaults

## Command Modes

## Supported User Roles

## Command History

Release	Modification

## Usage Guidelines

ssh6

## Examples

```
switch#
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:
```

Related Commands	Command	Description
	clear ssh session	
	ssh server enable	
	ssh6	

# ssh key

ssh key

no

ssh key dsa force rsa length force

no ssh key dsa rsa

## Syntax Description

dsa

force

rsa

*length*

## Defaults

## Command Modes

## Supported User Roles

## Command History

Release

Modification

## Usage Guidelines

ssh server enable no

## Examples

```
switch#
switch(config)#
generating dsa key(1024 bits).....
..
generated dsa key
```

```
switch#
switch(config)#
generating rsa key(1024 bits).....
.
generated rsa key
```

```
switch#
switch(config)# ssh key rsa 768
generating rsa key(768 bits).....
.
generated rsa key
```

```
switch# config t
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
deleting old dsa key.....
generating dsa key(1024 bits).....
.
generated dsa key
switch(config)# ssh server enable
```

```
switch# config t
switch(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
switch(config)# no ssh key dsa
switch(config)# ssh server enable
```

```
switch# config t
switch(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
switch(config)# no ssh key
switch(config)# ssh server enable
```

---

**Related Commands**

Command	Description
<b>show ssh key</b>	
<b>ssh server enable</b>	

---

# ssh server enable

ssh server enable

no

ssh server enable

no ssh server enable

---

## Syntax Description

---

## Defaults

---

## Command Modes

---

## Supported User Roles

---

## Command History

Release	Modification

---

## Usage Guidelines

---

## Examples

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

```
switch# config t
switch(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
```

---

## Related Commands

Command	Description
<b>show ssh server</b>	

# ssh6

ssh6

ssh6 @ vrf

## Syntax Description

---



---



---

vrf

---

## Defaults

## Command Modes

## Supported User Roles

## Command History

Release	Modification

## Usage Guidelines

ssh

## Examples

```
switch# ssh host2 vrf management
```

## Related Commands

Command	Description
clear ssh session	
ssh	
ssh server enable	

# statistics per-entry

MAC access control list (ACL), use the `statistics per-entry` command. To stop recording per-entry statistics, use the `no statistics per-entry` form of this command.

**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

**Supported User Roles** network-admin  
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(3)	Changed command from <code>statistics per-entry</code> to <code>statistics per-entry</code> .

**Usage Guidelines** When the device determines that an IPv4, IPv6, or MAC 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 `access-list` and `access-group` 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:

- 
- 
-

To view per-entry statistics for an ACL, use the command:

- 
- 
- 

command or the applicable following

To clear per-entry statistics for an ACL, use the following command:

- 
- 
- 

command or the applicable

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 t
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 t
switch(config)# ip access-list ip-acl-101
switch(config-acl)# no statistics per-entry
switch(config-acl)#
```

### Related Commands

Command	Description
	Displays all IPv4, IPv6, and MAC ACLs, or a specific ACL.
	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 storm-control` form of this command.

```
storm-control { broadcast | multicast | unicast } level [ . ]
```

**no storm-control { broadcast | multicast | unicast } level**

## Syntax Description

<b>broadcast</b>	Specifies the broadcast traffic.
<b>multicast</b>	Specifies the multicast traffic.
<b>unicast</b>	Specifies the unicast traffic.
	Percentage of the suppression level. The range is from 0 to 100 percent.
.	(Optional) Fraction of the suppression level. The range is from 0 to 99.

## Defaults

All packets are passed

## Command Modes

Interface configuration

## Supported User Roles

network-admin  
vdc-admin

## 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# config t  
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# config t  
switch(config)# interface ethernet 1/1  
switch(config-if)# no storm-control multicast level
```

---

**Related Commands**

Command	Description
<b>show interface</b>	Displays the storm-control suppression counters for an interface.
<b>show running-config</b>	Displays the configuration of the interface.

# switchport port-security

To enable port security on a Layer 2 interface, use the `switchport port-security` command. To remove port security configuration, use the `no switchport port-security` form of this command.

**Syntax Description** This command has no arguments or keywords.

**Defaults** None

**Command Modes** Interface configuration

**Supported User Roles** network-admin  
vdc-admin

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

**Usage Guidelines**

Per interface, port security is disabled by default.

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 sticky` command.

Port-security configuration is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

You must enable port security by using the `switchport port-security` command before you can use the `switchport port-security` command.

You must enable the interface using the `no shutdown` command before using this command.

This command does not require a license.

**Examples** This example shows how to enable port security on the Ethernet 2/1 interface:

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security
switch(config-if)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
	Enables port security globally.
	Shows information about port security.
	Configures the aging time for dynamically learned, secure MAC addresses.
	Configures the aging type for dynamically learned, secure MAC addresses.
	Configures a static MAC address.
	Enables the sticky method for learning secure MAC addresses.
	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
	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 `switchport port-security aging time default` form of this command.

<b>Syntax Description</b>	Specifies the 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.
---------------------------	--

<b>Defaults</b>	None
-----------------	------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Supported User Roles</b>	network-admin vdc-admin
-----------------------------	----------------------------

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

**Usage Guidelines**

The default aging time is 1440 minutes.

Port security configuration is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

You must enable port security by using the `switchport port-security` command before you can use the `switchport port-security aging time` command.

You must enable the interface using the `interface` command before using this command.

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

**Related Commands**

<b>Command</b>	<b>Description</b>
	Enables port security globally.
	Shows information about port security.
	Enables port security on a Layer 2 interface.
	Configures the aging type for dynamically learned, secure MAC addresses.
	Configures a static MAC address.
	Enables the sticky method for learning secure MAC addresses.
	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
	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 form of this command.

```
switchport port-security aging type { absolute | inactivity }
```

## Syntax Description

Specifies that the dynamically learned, secure MAC addresses age is based on how long ago the device learned the address.

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

## Command Modes

Interface configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The default aging type is absolute aging.

Port security configuration is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

You must enable port security by using the `switchport port-security` command before you can use the `switchport port-security aging type` command.

You must enable the interface using the `interface` command before using this command.

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# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security aging type inactivity
switch(config-if)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
	Enables port security globally.
	Shows information about port security.
	Configures a Layer 2 interface for port security.
	Configures the aging time for dynamically learned, secure MAC addresses.
	Configures a static MAC address.
	Enables the sticky method for learning secure MAC addresses.
	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
	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 switchport port-security mac-address` form of this command.

```
switchport port-security mac-address [ vlan-w ]
                                address [ vlan-ID ]
```

## Syntax Description

<i>address</i>	MAC address that you want to specify as a static, secure MAC address on the current interface.
<i>vlan-ID</i>	(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

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

There are no default static, secure MAC addresses.

Port security configuration is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

You must enable port security by using the `switchport port-security` command before you can use the `switchport port-security mac-address` command.

You must enable the interface using the `interface` command before using this command.

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# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE
switch(config-if)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
	Enables port security globally.
	Shows information about port security.
	Configures a Layer 2 interface for port security.
	Configures the aging time for dynamically learned, secure MAC addresses.
	Configures the aging type for dynamically learned, secure MAC addresses.
	Enables the sticky method for learning secure MAC addresses.
	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
	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 interface, use the `switchport port-security mac-address sticky` command. To disable the sticky method and return to the dynamic method, use the `switchport port-security mac-address dynamic` form of this command.

**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

**Supported User Roles** network-admin  
vdc-admin

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

**Usage Guidelines** Port security configuration is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

You must enable port security by using the `switchport port-security` command before you can use the `switchport port-security mac-address sticky` command.

You must enable the interface using the `interface ethernet` command before using this command.

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# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security mac-address sticky
switch(config-if)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
	Enables port security globally.
	Shows information about port security.
	Enables port security on a Layer 2 interface.
	Configures the aging time for dynamically learned, secure MAC addresses.
	Configures the aging type for dynamically learned, secure MAC addresses.
	Configures a static MAC address.
	Configures an interface or a VLAN maximum for secured MAC addresses on an interface.
	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 interface, use the `switchport port-security maximum` command. To remove port security configuration, use the `no switchport port-security maximum` form of this command.

```
switchport port-security maximum number [vlan-ID]
```

```
no switchport port-security maximum [vlan-ID]
```

## Syntax Description

<i>number</i>	Specifies the maximum number of secure MAC addresses. See the “Usage Guidelines” section for information about valid values for the <i>number</i> argument.
<i>vlan-ID</i>	(Optional) Specifies the VLAN that the maximum applies to. If you omit the keyword, the maximum is applied as an interface maximum.

## Defaults

None

## Command Modes

Interface configuration

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

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.

Port security configuration is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

You must enable port security by using the `switchport port-security` command before you can use the `switchport port-security maximum` command.

You must enable the interface using the `switchport mode access` command before using this command.

There is no default VLAN maximum.

There is a systemwide, 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# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security maximum 10
switch(config-if)#
```

### Related Commands

Command	Description
	Enables port security globally.
	Shows information about port security.
	Enables port security on a Layer 2 interface.
	Configures the aging time for dynamically learned, secure MAC addresses.
	Configures the aging type for dynamically learned, secure MAC addresses.
	Configures a static MAC address.
	Enables the sticky method for learning secure MAC addresses.
	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 port security violation action configuration, use the `no switchport port-security violation` form of this command.

```
switchport port-security violation {
    {
    }
}
```

## Syntax Description

Specifies that the device does not raise security violations when a packet would normally trigger a security violation event. Instead, the device allows address learning to continue until the maximum number of MAC addresses on the interface is reached, after which the device disables learning on the interface and drops all ingress traffic from non-secure MAC addresses.

Specifies that, after a security violation event, the device drops ingress traffic from any non-secure MAC addresses. The device keeps a count of the number of dropped packets.

Specifies that the device should shut 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

## Supported User Roles

network-admin  
vdc-admin

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The default security violation action is to shut down the interface.

Port security configuration is local to each virtual device context (VDC). If necessary, switch to the correct VDC before using this command.

You must enable port security by using the `switchport port-security` command before you can use the `switchport port-security violation` command.

You must enable the interface using the `no shutdown` command before using this command.

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:

-

-

-

-

- 



---

**Note**

---

- 

- 

- 

---

**Examples**

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security violation protect
switch(config-if)#
```

