Configuring Port Security

This chapter contains the following sections:

Information About Port Security

Port security allows you to configure Layer 2 interfaces that permit inbound traffic from a restricted, secured set of MAC addresses. Traffic from secured MAC addresses is not allowed on another interface within the same VLAN. The number of MAC addresses that can be secured is configured per interface.

Secure MAC Address Learning

The following information describes secure MAC address learning:

- The process of securing a MAC address is called learning.
- The number of addresses that can be learned is restricted.
- Address learning can be accomplished on any interface where port security is enabled.

Static Method

- The static learning method allows you to manually add or remove secure MAC addresses to the running configuration of an interface. If you copy the running configuration to the startup configuration, static secure MAC addresses are persistent if the device restarts.
- A static secure MAC address entry remains in the configuration of an interface until you explicitly remove the address from the configuration.

- Adding secure addresses by the static method is not affected by whether dynamic or sticky address learning is enabled.
- The burned-in MAC address is secured as a static MAC address starting from Release 5.2(1)SV3(1.1). In previous releases, the burned-in MAC address was secured as a dynamic MAC address.

Dynamic Method

By default, when you enable port security on an interface, you enable the dynamic learning method. With this method, the device secures MAC addresses as ingress traffic passes through the interface. If the address is not yet secured and the device has not reached any applicable maximum, it secures the address and allows the traffic.

The device stores dynamic secure MAC addresses in memory. A dynamic secure MAC address entry remains in the configuration of an interface until one of the following events occurs:

- The VSM and VEM restarts.
- The interface restarts.
- The address reaches the age limit that you configured for the interface.
- You explicitly remove the address.

The burned-in MAC address is secured as a static MAC address starting from Release 5.2(1)SV3(1.1). In previous releases, the burned-in MAC address was secured as a dynamic MAC address.

Sticky Method

- If you enable the sticky method, the device secures MAC addresses in the same manner as dynamic address learning. These addresses can be made persistent through a reboot by using the **copy run start** command to copy the running configuration to the startup configuration.
- Dynamic and sticky address learning are mutually exclusive. When you enable sticky learning on an interface, dynamic learning is stopped and sticky learning is used instead. If you disable sticky learning, dynamic learning is resumed.
- Sticky secure MAC addresses are not aged.
- A sticky secure MAC address entry remains in the configuration of an interface until you explicitly remove the address.

Dynamic Address Aging

MAC addresses that are learned by the dynamic method are aged and dropped when reaching the age limit. You can configure the age limit on each interface. The range is from 0 to 1440 minutes, where 0 disables aging.

There are two methods of determining the address age:

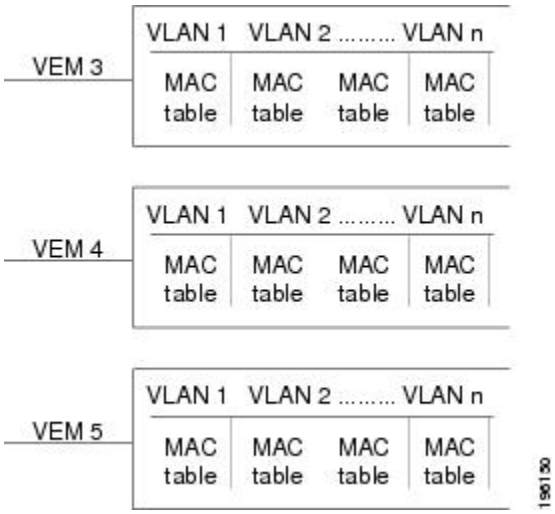
- Inactivity—The length of time after the device last received a packet from the address on the applicable interface.
- Absolute—The length of time after the device learned the address. This is the default aging method; however, the default aging time is 0 minutes, which disables aging.

Secure MAC Address Maximums

The secure MAC addresses on a secure port are inserted in the same MAC address table as other regular MAC addresses. If a MAC table has reached its limit, it does not learn any new secure MAC addresses for that VLAN.

The following figure shows that each VLAN in a VEM has a forwarding table that can store a maximum number of secure MAC addresses.

Figure 1: Secure MAC Addresses per VEM



Interface Secure MAC Addresses

By default, an interface can have only one secure MAC address. You can configure the maximum number of MAC addresses permitted per interface or per VLAN on an interface. Maximums apply to secure MAC addresses learned by any method: dynamic, sticky, or static.

The following limits can determine how many secure MAC address are permitted on an interface:

- Device maximum— If learning a new address would violate the device maximum, the device does not permit the new address to be learned, even if the interface or VLAN maximum has not been reached.
- Interface maximum—You can configure a maximum number of secure MAC addresses for each interface protected by port security. The default interface maximum is one address for both access and trunk vethernet ports. Interface maximums cannot exceed the device maximum.
- VLAN maximum—You can configure the maximum number secure MAC addresses per VLAN for each interface protected by port security. A VLAN maximum cannot exceed the interface maximum. VLAN maximums are useful only for trunk ports. There are no default VLAN maximums.

The maximum number of secure MAC addresses per port is limited to ten. When configuring ports in trunk mode, be sure not to exceed the maximum MAC address limit.

You can configure a VLAN and interface maximums per interface, as needed; however, when the new limit is less than the applicable number of secure addresses, you must reduce the number of secure MAC addresses first.

Security Violations and Actions

Port security triggers a security violation when the following occurs:

Note Beginning with Release 5.2(1)SV3(1.1), MAC move detection and violation is local to a VEM.

- 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 five addresses.
  - The interface has a maximum of ten addresses.

  A violation is detected when either of the following occurs:

  - Five addresses are learned for VLAN 1 and inbound traffic from a sixth address arrives at the interface in VLAN 1.
  - Ten addresses are learned on the interface and inbound traffic from an 11th address arrives at the interface.

When a security violation occurs on an interface, the action specified in its port security configuration is applied. The possible actions that the device can take 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.

  ```
  switch(config)# errdisable recovery cause psecure-violation
  switch(config)# copy running-config startup-config
  ```

- Protect—Prevents violations from occurring. Address learning continues 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 nonsecure MAC addresses.
- Restrict—Prevents violations from occurring. Address learning continues 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 nonsecure MAC addresses and causes the security violation counter to increment.

Port Security and Port Types

You can configure port security only on Layer 2 interfaces. Details about port security and different types of interfaces or ports are as follows:

- Access ports—You can configure port security on interfaces that you have configured as Layer 2 access ports. On an access port, port security applies only to the access VLAN.
- Trunk ports—You can configure port security on interfaces that you have configured as Layer 2 trunk veth ports. VLAN maximums are not useful for access ports. The device allows VLAN maximums only for VLANs associated with the trunk port.
- SPAN ports—You can configure port security on SPAN source ports but not on SPAN destination ports.
- Ethernet Ports—Port security is not supported on Ethernet ports.
- Ethernet Port Channels—Port security is not supported on Ethernet port channels.

Result of Changing an Access Port to a Trunk Port

When you change a Layer 2 interface from an access port to a trunk port, the device drops all secure addresses learned by the dynamic method. The device moves the addresses learned by the static or sticky method to the native trunk VLAN.

Result of Changing a Trunk Port to an Access Port

When you change a Layer 2 interface from a trunk port to an access port, the device drops all secure addresses learned by the dynamic method. It also moves all addresses learned by the sticky method on the native trunk VLAN to the access VLAN. The device drops secure addresses learned by the sticky method if they are not on the native trunk VLAN.

Beginning with Release 5.2(1)SV3(1.1), the maximum number of secure MAC addresses per port is limited to 10. When configuring ports in trunk mode, be sure not to exceed the maximum MAC address limit. If you configure an interface in trunk mode that exceeds the MAC address limit and you attempt to change the mode to access, the interface might be left with stale secure MAC address entries.

Guidelines and Limitations for Port Security

- Port security is not supported on the following:
  - Ethernet interfaces
  - Ethernet port-channel interfaces
  - Switched port analyzer (SPAN) destination ports
- Port security cannot be configured on interfaces with existing static MAC addresses.
- Port security cannot be enabled on interfaces whose VLANs have an existing static MAC address even if it is programmed on a different interface.
- If the interface maximum has been reached for secure MAC addresses and you add an additional static MAC address, the interface enters error-disable mode. To enable the interface, you must first remove the static MAC address using the **no switchport port-security mac-address** command and then use the **shutdown** and **no shutdown** commands on the interface. To avoid this issue, before adding additional static MAC addresses, use the **show port-security address interface** *veth-number* command to verify whether the interface maximum has been reached.

- Beginning with Release 5.2(1)SV3(1.1), the maximum number of secure MAC addresses per port is limited to 10. When configuring ports in trunk mode, be sure not to exceed the maximum MAC address limit. If you configure an interface in trunk mode that exceeds the MAC address limit and you attempt to change the mode to access, the interface might be left with stale secure MAC address entries.

Default Settings for Port Security

Parameters	Default
Interface	Disabled
MAC address learning method	Dynamic
Interface maximum number of secure MAC addresses	1
Security violation action	Shutdown

Configuring Port Security

Enabling or Disabling Port Security on a Layer 2 Interface

You can enable or disable port security on a Layer 2 interface.

By default, port security is disabled on all interfaces.

Enabling port security on an interface also enables dynamic MAC address learning.

Before you begin

- Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type number*	Places you into interface configuration mode for the specified interface.
Step 3	switch(config-if)# [**no**] **switchport port-security**	Enables port security on the interface. Using the **no** option disables port security on the interface.
Step 4	switch(config-if)# **show port-security address interface vethernet number**	Displays the secure MAC address learnt on the interface.

	Command or Action	Purpose
Step 5	switch(config-if)# **show port-security interface vethernet number**	Displays the port security configuration on the interface.
Step 6	(Optional) switch(config-if)# **show running-config port-security**	Displays the port security configuration.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to enable port security on a Layer 2 interface:

```
switch# configure terminal
switch(config)# interface vethernet 36
switch(config-if)# switchport port-security
switch(config-if)# show running-config port-security
interface Vethernet36
switchport port-security
switch(config-if)# show port-security address interface vethernet 36
Secure Mac Address Table
------------------------------------------------------------------------
Vlan Mac Address Type Ports Configured Age
(mins)
---- ----------- ------ ----- ---------------
2303 0050.5687.3C68 DYNAMIC Vethernet36 0
------------------------------------------------------------------------
switch(config-if)# show port-security interface vethernet 36
Port Security : Enabled
Port Status : Secure UP
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Security violation count : 0

switch(config-if)# copy running-config startup-config
```

Enabling or Disabling Sticky MAC Address Learning

You can enable or disable sticky MAC address learning.

Dynamic MAC address learning is the default on an interface.

By default, sticky MAC address learning is disabled.

Before you begin

- Log in to the CLI in EXEC mode.
- Enable port security on the interface that you are configuring.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type number*	Places you into interface configuration mode for the specified interface.
Step 3	switch(config-if)# [**no**] **switchport port-security mac-address sticky**	Enables sticky MAC address learning on the interface. Using the **no** option disables sticky MAC address learning.
Step 4	switch(config-if)# **show port-security address interface vethernet number**	Displays the secure MAC address learnt on the interface.
Step 5	switch(config-if)# **show port-security interface vethernet number**	Displays the port security configuration on the interface.
Step 6	(Optional) switch(config-if)# **show running-config port-security**	Displays the port security configuration.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to enable sticky MAC address learning:

```
switch(config)# interface Vethernet36
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security mac-address sticky
switch(config-if)# switchport port-security mac-address 0050.5687.3C4B
switch(config)# show running-config port-security
interface Vethernet36
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address 0050.5687.3C4B
switch(config)# show port-security address interface vethernet 36
Secure Mac Address Table
------------------------------------------------------------------------
Vlan Mac Address Type Ports Configured Age
(mins)
---- ----------- ------ ----- ---------------
2304 0050.5687.3C4B STICKY Vethernet36 0
------------------------------------------------------------------------
```

Adding a Static Secure MAC Address on an Interface

You can add a static secure MAC address on an interface.

By default, no static secure MAC addresses are configured on an interface.

Before you begin

- Log in to the CLI in EXEC mode.
- Determine if the interface maximum has been reached for secure MAC addresses. If the interface maximum has been reached for secure MAC addresses and you add an additional static MAC address, the interface enters error-disable mode. To enable the interface, you must first remove the static MAC address using the **no switchport port-security mac-address** command and then use the **shutdown** and **no shutdown** commands on the interface. To avoid this issue, before adding additional static MAC addresses, use the **show port-security address interface** *veth-number* command to verify whether the interface maximum has been reached.
- Enable port security on the interface that you are configuring.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type number*	Places you into interface configuration mode for the specified interface.
Step 3	switch(config-if)# [**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*]	Configures a static MAC address for port security on the current interface. Use the **vlan** keyword if you want to specify the VLAN that traffic from the address is allowed on.
Step 4	switch(config-if)# **show port-security address interface vethernet number**	Displays the secure MAC address learnt on the interface.
Step 5	switch(config-if)# **show port-security interface vethernet number**	Displays the port security configuration on the interface.
Step 6	(Optional) switch(config-if)# **show running-config port-security**	Displays the port security configuration.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to add a static secure MAC address on an interface:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 2
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security mac-address 0019.0002.0102
switch(config-if)# show running-config port-security

!Command: show running-config port-security
!Time: Tue Aug 12 23:49:23 2014

version 5.2(1)SV3(1.1)
```

```
interface Vethernet2
switchport port-security
switchport port-security maximum 5
switchport port-security mac-address 0019.0002.0102

switch(config-if)# show port-security address interface vethernet 2
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.1f1c STATIC Vethernet2 0
51 0019.0002.0102 STATIC Vethernet2 0
switch(config-if)# copy running-config startup-config
```

Removing a Static or a Sticky Secure MAC Address from an Interface

Starting in Release #5.2(1)SV3(1.1), the Sticky MAC address is stored only on the Virtual Ethernet Module (VEM) and not on the Virtual Supervisor Module (VSM). The stored MAC addresses that are secured using Sticky MAC address configuration do not persist across events such as **vMotions**, **Port Group Change**, and **Interface Disconnect from VC**.

Before you begin

- Log in to the CLI in EXEC mode.
- Enable port security on the interface that you are configuring.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type number*	Places you into interface configuration mode for the specified interface.
Step 3	switch(config-if)# **no switchport port-security mac-address** *address*	Removes the MAC address from port security on the current interface.
Step 4	switch(config-if)# **show port-security address interface vethernet number**	Displays the secure MAC address learnt on the interface.
Step 5	switch(config-if)# **show port-security interface vethernet number**	Displays the port security configuration on the interface.
Step 6	(Optional) switch(config-if)# **show running-config port-security**	Displays the port security configuration.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to remove the MAC address from port security on the current interface:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 2
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security mac-address 0019.0002.0102
switch(config-if)# show port-security address interface vethernet 2
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.1f1c STATIC Vethernet2 0
51 0019.0002.0102 STATIC Vethernet2 0
switch(config-if)# no switchport port-security mac-address 0019.0002.0102
switch(config-if)# show port-security address interface vethernet 2
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.1f1c STATIC Vethernet2 0
switch(config-if)# copy running-config startup-config
```

Removing a Dynamic Secure MAC Address

You can remove a specific address learned by the dynamic method or remove all addresses learned by the dynamic method on a specific interface.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **clear port-security dynamic** {**interface vethernet** *number* | **address** *address* | **module** *module-numbef*} [**vlan** *vlan-ID*]	Removes dynamically learned, secure MAC addresses, as specified. The keywords are as follows: • **interface**—Removes all dynamically learned addresses on the interface that you specify. • **address**—Removes the single, dynamically learned address that you specify. • **module**—Removes all dynamically learned addresses on the specified module.

	Command or Action	Purpose
		• **vlan**—Removes an address or addresses on a particular VLAN.
Step 3	(Optional) switch(config)# **show port-security address**	Displays secure MAC addresses.

Example

This example shows how to remove a dynamically learned, secure MAC address by specifying the vethernet number:

```
switch(config)# show port-security address interface vethernet 2
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.1f1c STATIC Vethernet2 0
51 0010.0201.0500 DYNAMIC Vethernet2 0
switch(config)# clear port-security dynamic interface vethernet 2
switch(config)# show port-security address interface vethernet 2
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.1f1c STATIC Vethernet2 0
switch(config)#
```

This example shows how to remove a dynamically learned, secure MAC address by specifying the module number:

```
switch(config)# show port-security address interface vethernet 2
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.1f1c STATIC Vethernet2 0
51 0010.0201.0500 DYNAMIC Vethernet2 0

switch(config)# clear port-security dynamic address 0010.0201.0500 module 3
switch(config)# show port-security address interface vethernet 2
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.1f1c STATIC Vethernet2 0
switch(config)#
```

Configuring a Maximum Number of MAC Addresses

You can configure the maximum number of MAC addresses that can be learned or statically configured on a Layer 2 interface. You can also configure a maximum number of MAC addresses per VLAN on a Layer 2 interface.

The secure MAC addresses share the Layer 2 Forwarding Table (L2FT). The forwarding table for each VLAN can hold up to 10 entries.

By default, an interface has a maximum of one secure MAC address.

VLANs have no default maximum number of secure MAC addresses.

To remove all addresses learned by the dynamic method, use the **shutdown** and **no shutdown** commands to restart the interface.

Note When you specify a maximum number of addresses that is less than the number of addresses already learned or statically configured on the interface, the command is rejected.

Before you begin

- Log in to the CLI in EXEC mode.
- Enable port security on the interface that you are configuring.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type number*	Places you into interface configuration mode for the specified interface.
Step 3	switch(config-if)# [**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*]	Configures the maximum number of MAC addresses that can be learned or statically configured for the current interface. The **no** option resets the maximum number of MAC addresses to the default, which is 1. If you want to specify the VLAN that the maximum applies to, use the **vlan** keyword. **Note** The maximum number of MAC addresses that can be secured on an interface is ten. However, the command allows you to configure 1,025. We recommend that you do not configure more than ten.
Step 4	switch(config-if)# **show port-security address interface vethernet number**	Displays the secure MAC address learnt on the interface.

	Command or Action	Purpose
Step 5	switch(config-if)# **show port-security interface vethernet number**	Displays the port security configuration on the interface.
Step 6	(Optional) switch(config-if)# **show running-config port-security**	Displays the port security configuration.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration. **Note** The VLAN ID configuration is not supported on access port and is only applicable to trunk ports.

Example

This example shows how to configure a maximum number of MAC addresses:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 2
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security maximum 5
switch(config-if)# show port-security interface vethernet 2
Port Security : Enabled
Violation Mode : Shutdown
Aging Time : 0
Aging Type : Absolute
Maximum MAC Addresses : 5
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Security violation count : 0
switch(config-if)# show running-config port-security

!Command: show running-config port-security
!Time: Wed Aug 13 00:56:49 2014

version 5.2(1)SV3(1.1)

interface Vethernet2
switchport port-security
switchport port-security maximum 5

switch(config-if)# copy running-config startup-config
```

Configuring an Address Aging Type and Time

You can configure the MAC address aging type and the length of time used to determine when MAC addresses learned by the dynamic method have reached their age limit.

There are two methods for determining address aging:

- Inactivity—The length of time after the device last received a packet from the address on the applicable interface.
- Absolute—The length of time after the device learned the address. This is the default aging method; however, the default aging time is 0 minutes, which disables aging.

Before you begin

- Log in to the CLI in EXEC mode.
- Enable port security on the interface that you are configuring.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type number*	Places you into interface configuration mode for the specified interface.
Step 3	switch(config-if)# [**no**] **switchport port-security aging type** {**absolute** | **inactivity**}	Configures the type of aging that the device applies to dynamically learned MAC addresses. The **no** option resets the aging type to the default, which is absolute aging.
Step 4	switch(config-if)# [**no**] **switchport port-security aging time** *minutes*	Configures the number of minutes that a dynamically learned MAC address must age before the address is dropped. The maximum valid minutes is 1440. The **no** option resets the aging time to the default, which is 0 minutes (no aging).
Step 5	(Optional) switch(config-if)# **show port-security address interface vethernet number**	Displays the secure MAC address learnt on the interface.
Step 6	(Optional) switch(config-if)# **show port-security interface vethernet number**	Displays the port security configuration on the interface.
Step 7	(Optional) switch(config-if)# **show running-config port-security**	Displays the port security configuration.
Step 8	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure an address aging type and time:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 3
switch(config-if)# switchport port-security
```

```
switch(config-if)# switchport port-security aging type inactivity
switch(config-if)# switchport port-security aging time 120
switch(config-if)# show port-security address interface vethernet 3
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.38ec STATIC Vethernet3 0
51 0000.0000.0010 DYNAMIC Vethernet3 120
switch(config-if)# show port-security interface vethernet 3
Port Security : Enabled
Violation Mode : Shutdown
Aging Time : 120
Aging Type : Inactivity
Maximum MAC Addresses : 5
Total MAC Addresses : 2
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Security violation count : 0
switch(config-if)# copy running-config startup-config
switch(config-if)# show running-config port-security

!Command: show running-config port-security
!Time: Wed Aug 13 01:06:00 2014

version 5.2(1)SV3(1.1)

interface Vethernet3
switchport port-security
switchport port-security aging type inactivity
switchport port-security aging time 120
switchport port-security maximum 5
```

Configuring a Security Violation Action

You can configure how an interface responds to a security violation. You can configure the following interface responses to security violations:

- **protect**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
- **restrict**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the SecurityViolation counter to increment.
- **shutdown** (the default)—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

Before you begin

- Log in to the CLI in EXEC mode.
- Enable port security on the interface that you are configuring.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface** *type number*	Places you into interface configuration mode for the specified interface.
Step 3	switch(config-if)# [**no**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**}	Configures the security violation action for port security on the current interface. The **no** option resets the violation action to the default, which is to shut down the interface. The keywords are as follows: • **protect**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value • **restrict**—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value, which increments the Security Violation counter. • **shutdown** (the default)—Puts the interface into the error-disabled state immediately and sends an SNMP trap notification and syslog event.
Step 4	switch(config-if)# **show port-security address interface vethernet number**	Displays the secure MAC address learnt on the interface.
Step 5	switch(config-if)# **show port-security interface vethernet number**	Displays the port security configuration on the interface.
Step 6	(Optional) switch(config-if)# **show running-config port-security**	Displays the port security configuration.
Step 7	(Optional) switch(config-if)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

This example shows how to configure a security violation action:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 3
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security violation protect
```

```
switch(config-if)# show port-security interface vethernet 3
Port Security : Enabled
Violation Mode : Protect
Aging Time : 120
Aging Type : Inactivity
Maximum MAC Addresses : 5
Total MAC Addresses : 2
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Security violation count : 0
# copy running-config startup-config

switch(config-if)# show running-config port-security

!Command: show running-config port-security
!Time: Wed Aug 13 01:14:41 2014

version 5.2(1)SV3(1.1)

interface Vethernet3
switchport port-security
switchport port-security aging type inactivity
switchport port-security aging time 120
switchport port-security maximum 5
switchport port-security violation protect
```

Recovering Ports Disabled for Port Security Violations

You can automatically recover an interface disabled for port security violations. To recover an interface manually from the error-disabled state, you must enter the **shutdown** command and then the **no shutdown** command.

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **errdisable recovery cause psecure-violation**	Enables a timed automatic recovery of the specified port that is disabled for a port security violation.
Step 3	switch(config)# **errdisable recovery interval** *seconds*	Configures a timer recovery interval in seconds from 30 to 65535 seconds.

Example

This example shows how to recover ports that are disabled for port security violations:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# errdisable recovery cause psecure-violation
switch(config)# errdisable recovery interval 30
switch(config)# copy running-config startup-config
switch(config)# show errdisable recovery
ErrDisable Reason Timer Status
----------------- ------------
link-flap disabled
bpduguard disabled
dhcp-rate-limit enabled
arp-inspection enabled
security-violation disabled
psecure-violation enabled
failed-port-state enabled
ip-addr-conflict disabled

Timer interval: 30
```

Verifying the Port Security Configuration

Use the following commands to verify the configuration:

Command	Purpose
show running-config port-security	Displays the port security configuration.
show port-security address interface vethernet number	Displays the secure MAC address learnt on the interface.
show port-security interface vethernet number	Displays the port security configuration on the interface.

Displaying Secure MAC Addresses

Use the **show port-security address** command to display secure MAC addresses.

Configuration Example for Port Security

This example shows a port security configuration for the vEthernet 3 interface with a VLAN and interface maximums for secure addresses. In this example, the interface is a trunk port. Additionally, the violation action is set to protect.

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 3
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security maximum 10
switch(config-if)# switchport port-security maximum 6 vlan 50
switch(config-if)# switchport port-security maximum 3 vlan 55
switch(config-if)# switchport port-security violation protect
```

```
switch(config-if)# switchport mode trunk
switch(config-if)# show running-config interface vethernet 3
interface Vethernet3
switchport mode trunk
switchport port-security
switchport port-security maximum 10
switchport port-security violation protect
switchport port-security maximum 6 vlan 50
switchport port-security maximum 3 vlan 55
switch(config)# copy running-config startup-config
```

The following example shows a port security configuration for the vEthernet 3 interface as an access port with an interface maximum set to 10, a violation set to restrict, an absolute timeout of 1 minute and a port security static MAC address of 0000.1111.5555:

```
switch(config)# interface vethernet 3
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security aging time 1
switch(config-if)# switchport port-security aging type absolute
switch(config-if)# switchport port-security maximum 10
switch(config-if)# switchport port-security mac-address 0000.1111.5555
switch(config-if)# switchport port-security violation restrict
switch(config-if)# show running-config interface vethernet 3
interface Vethernet3
switchport port-security
switchport port-security aging time 1
switchport port-security maximum 10
switchport port-security violation restrict
switchport port-security mac-address 0000.1111.5555
switchport port-security aging type absolute
no shutdown

switch(config-if)# show port-security interface vethernet 3
Port Security : Enabled
Violation Mode : Restrict
Aging Time : 1
Aging Type : Absolute
Maximum MAC Addresses : 10
Total MAC Addresses : 7
Configured MAC Addresses : 7
Sticky MAC Addresses : 0
Security violation count : 0
switch(config-if)# copy running-config startup-config
```

This example shows a port security configuration for the vEthernet 3 interface as an access port with a violation set to shutdown, maximum count to 2 and MAC address learning set to sticky:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 3
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security mac-address sticky
switch(config-if)# switchport port-security violation shutdown
switch(config-if)# switchport port-security maximum 2
switch(config-if)# show running-config interface vethernet 3
interface Vethernet3
inherit port-profile 51
switchport port-security violation shutdown
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switch(config-if)# show port-security interface vethernet 3
Port Security : Enabled
```

```
Violation Mode : Shutdown
Aging Time : 0
Aging Type : Absolute
Maximum MAC Addresses : 2
Total MAC Addresses : 2
Configured MAC Addresses : 1
Sticky MAC Addresses : 1
Security violation count : 0
switch(config-if)# show port-security address interface vethernet 3
Secure Mac Address Table
------------------------------------------------------------------------
Vlan/Vxlan Mac Address Type Ports Configured Age
(mins)
---------- ----------- ------ ----- ---------------
51 0050.56a4.38ec STATIC Vethernet3 0
51 0000.0000.0010 STICKY Vethernet3 0
switch(config-if)# copy running-config startup-config
```

Feature History for Port Security

This table only includes updates for those releases that have resulted in additions to the feature.

Feature Name	Releases	Feature Information
MAC address per port limit	5.2(1)SV3(1.1)	The maximum number of secure MAC addresses per port is limited to ten.
MAC Move Detection and Violation	5.2(1)SV3(1.1)	This feature is now local to VEM.
Port Security	4.0(4)SV1(1)	This feature was introduced.