



Configuring Port Security

This chapter includes the following sections:

- [Information About Port Security, on page 1](#)
- [Licensing Requirements for Port Security, on page 6](#)
- [Prerequisites for Port Security, on page 6](#)
- [Guidelines and Limitations for Port Security, on page 6](#)
- [Guidelines and Limitations for Port Security on vPCs, on page 7](#)
- [Default Settings for Port Security, on page 7](#)
- [Configuring Port Security, on page 8](#)
- [Verifying the Port Security Configuration, on page 18](#)
- [Displaying Secure MAC Addresses, on page 18](#)
- [Configuration Example for Port Security, on page 18](#)
- [Configuration Example of Port Security in a vPC Domain, on page 19](#)
- [Additional References for Port Security, on page 19](#)

Information About Port Security

Port security allows you to configure Layer 2 physical interfaces and Layer 2 port-channel interfaces to allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, the device does not allow traffic from these MAC addresses on another interface within the same VLAN. The number of MAC addresses that the device can secure is configurable per interface.



Note

Unless otherwise specified, the term *interface* refers to both physical interfaces and port-channel interfaces; physical interfaces, port-channel interfaces, and vPCs; likewise, the term *Layer 2 interface* refers to both Layer 2 physical interfaces and Layer 2 port-channel interfaces.

Secure MAC Address Learning

The process of securing a MAC address is called learning. A MAC address can be a secure MAC address on one interface only. For each interface that you enable port security on, the device can learn a limited number

of MAC addresses by the static, dynamic, or sticky methods. The way that the device stores secure MAC addresses varies depending upon how the device learned the secure MAC address.

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 unaffected if the device restarts.

A static secure MAC address entry remains in the configuration of an interface until one of the following events occurs:

- You explicitly remove the address from the configuration.
- You configure the interface to act as a Layer 3 interface.

Adding secure addresses by the static method is not affected by whether dynamic or sticky address learning is enabled.

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 secured on an interface until one of the following events occurs:

- The device restarts.
- The interface restarts.
- The address reaches the age limit that you configured for the interface.
- You explicitly remove the address. For more information, see [Removing a Dynamic Secure MAC Address, on page 14](#).
- You configure the interface to act as a Layer 3 interface.

Sticky Method

If you enable the sticky method, the device secures MAC addresses in the same manner as dynamic address learning, but the device stores addresses learned by this method in nonvolatile RAM (NVRAM). As a result, addresses learned by the sticky method persist through a device restart. Sticky secure MAC addresses do not appear in the running configuration of an interface.

Dynamic and sticky address learning are mutually exclusive. When you enable sticky learning on an interface, the device stops dynamic learning and performs sticky learning instead. If you disable sticky learning, the device resumes dynamic learning.

A sticky secure MAC address entry remains secured on an interface until one of the following events occurs:

- You explicitly remove the sticky MAC address configuration from the interface. For more information, see [Removing a Sticky Secure MAC Address, on page 13](#).
- You configure the interface to act as a Layer 3 interface.

Dynamic Address Aging

The device ages MAC addresses learned by the dynamic method and drops them after the age limit is reached. You can configure the age limit on each interface. The range is from 1 to 1440 minutes. The default aging time is 0, which disables aging.

The method that the device uses to determine that the MAC address age is also configurable. The two methods of determining address age are as follows:

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.

**Note**

If the absolute method is used to age out a MAC address, then depending on the traffic rate, few packets may drop each time a MAC address is aged out and relearned. To avoid this use inactivity timeout.

Secure MAC Address Maximums

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.

**Note**

In vPC domains, the configuration on the primary vPC takes effect.

**Tip**

To ensure that an attached device has the full bandwidth of the port, set the maximum number of addresses to one and configure the MAC address of the attached device.

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

System maximum

The device has a nonconfigurable limit of 8192 secure MAC addresses. 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 1025 secure MAC addresses for each interface protected by port security. The default interface maximum is one address. Sum of all interface maximums on a switch cannot exceed the system maximum.

VLAN maximum

You can configure the maximum number of secure MAC addresses per VLAN for each interface protected by port security. The sum of all VLAN maximums under an interface cannot exceed the configured

interface maximum. VLAN maximums are useful only for trunk ports. There are no default VLAN maximums.

You can configure 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. Otherwise, the configuration of new limit is rejected.

Security Violations and Actions

Port security triggers security violations when either of the two following events occur:

MAX Count Violation

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 20 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.
-

MAC Move Violation

Ingress traffic from a secure MAC address arrives at a different secured interface in the same VLAN as the interface on which the address is secured.

When a security violation occurs, the device increments the security violation counter for the interface and takes the action specified by the port security configuration of the interface. 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.

The violation modes and the possible actions that a device can take are as follows:

Shutdown violation mode

Error disables the interface that received the packet triggering the violation and the port shuts down. The security violation count is set to 1. This action is the default. After you reenables the interface, it retains its port security configuration, including its static and sticky secure MAC addresses. However, the dynamic MAC addresses are not retained and have to be relearned.

You can use the **errdisable recovery cause psecure-violation** global configuration command to configure the device to reenables the interface automatically if a shutdown occurs, or you can manually reenables the interface by entering the **shutdown** and **no shut down** interface configuration commands. For detailed information about the commands, see the Security Command Reference for your platform.

Restrict violation mode

Drops ingress traffic from any nonsecure MAC addresses.

The device keeps a count of the number of unique source MAC addresses of dropped packets, which is called the security violation count.

Violation is triggered for each unique nonsecure source MAC address and security violation count increments till 10, which is the maximum value. The maximum value of 10 is fixed and not configurable.

Address learning continues until the maximum security violations (10 counts) have occurred on the interface. Traffic from addresses learned after the first security violation are added as BLOCKED entries in the MAC table and dropped. These BLOCKED MAC address age out after 5 minutes. The BLOCKED MAC address age out time of 5 minutes is fixed and not configurable.

Depending on the violation type, RESTRICT mode action varies as follows:

- In case of MAX count violation, after the maximum number of MAX count violations (10) is reached, the device stops learning new MAC addresses. Interface remains up.
- In case of MAC move violation, when the maximum security violations have occurred on the interface, the interface is error Disabled.

Protect violation mode

Prevents further violations from occurring. The address that triggered the security violation is learned but any traffic from the address is dropped. Security violation counter is set to 1, which is the maximum value. Further address learning stops. Interface remains up.

Note that the security violation is reset to 0 after the interface is recovered from violation through one of the following events:

- Dynamic secure MAC addresses age out
- Interface flap, link down, or link up events
- Port-security disable and re-enable on the interface
- Changing violation mode of the interface



Note If an interface is errDisabled, you can bring it up only by flapping the interface.

Port Type Changes

When you have configured port security on a Layer 2 interface and you change the port type of the interface, the device behaves as follows:

Access port to trunk port

When you change a Layer 2 interface from an access port to a trunk port, the device deletes all secure addresses learned by the dynamic method. The device moves the addresses learned by the static method to the native trunk VLAN. The sticky MAC addresses remain in same VLAN if the VLAN exists. Otherwise, the MAC addresses move to the native VLAN of the trunk port.

Trunk port to 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.

Switched port to routed port

When you change an interface from a Layer 2 interface to a Layer 3 interface, the device disables port security on the interface and discards all port security configuration for the interface. The device also discards all secure MAC addresses for the interface, regardless of the method used to learn the address.

Routed port to switched port

When you change an interface from a Layer 3 interface to a Layer 2 interface, the device has no port security configuration for the interface.

The static secure addresses that are configured per access or trunk VLAN on an interface are not retained during the following events:

- Changing global VLAN mode of the active VLANs on an interface between classical Ethernet and fabric path interfaces
- Changing switchport mode access or trunk to private VLAN or vice versa

Licensing Requirements for Port Security

The following table shows the licensing requirements for this feature:

| Product | License Requirement |
|-------------|---|
| Cisco NX-OS | Port security requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS device images and is provided at no extra charge to you. |

Prerequisites for Port Security

Guidelines and Limitations for Port Security

When configuring port security, follow these guidelines:

- Port security is supported on PVLAN ports.
- Port security does not support switched port analyzer (SPAN) destination ports.
- Port security does not depend upon other features.
- If any member link in a port-channel is in the pre-provisioned state, that is, the module is offline, then the port security feature cannot be disabled on the port-channel.

Guidelines and Limitations for Port Security on vPCs

In addition to the guidelines and limitations for port security, there are additional guidelines and limitations for port security on vPCs. When configuring port security on vPCs, follow these guidelines:

- You must enable port security globally on both vPC peers in a vPC domain.
- You must enable port security on the vPC interfaces of both vPC peers.
- You must configure a static secure MAC address on the primary vPC peer. This MAC address is synchronized with the secondary vPC peer. You can also configure a static secure MAC address on the secondary peer. This MAC address appears in the secondary vPC configuration, but does not take effect.
- All learned MAC addresses are synchronized between vPC peers.
- Both vPC peers can be configured with either the dynamic or sticky MAC address learning method. However, we recommend that both vPC peers be configured for the same method.
-
- Dynamic MAC addresses are dropped only after the age limit is reached on both vPC peers.
- You set the maximum number of secure MAC addresses on the primary vPC switch. The primary vPC switch does the count validation, even if a maximum number of secure MAC addresses is set on the secondary switch.
- You configure the violation action on the primary vPC. So, whenever a security violation is triggered, the security action defined on the primary vPC switch occurs.
- Port security is enabled on a vPC interface when the port security feature is enabled on both vPC peers and port security is enabled on both vPC interfaces of the vPC peers. You can use the **config sync** command to verify that the configuration is correct.
- While a switch undergoes an in-service software upgrade (ISSU), port security operations are stopped on its peer switch. The peer switch does not learn any new MAC addresses, and MAC moves occurring during this operation are ignored. When the ISSU is complete, the peer switch is notified and normal port security functionality resumes.
- ISSU to higher versions is supported; however ISSU to lower versions is not supported.

Default Settings for Port Security

This table lists the default settings for port security parameters.

Table 1: Default Port Security Parameters

| Parameters | Default |
|--|----------|
| Port security enablement globally | Disabled |
| Port security enablement per interface | Disabled |
| MAC address learning method | Dynamic |

| Parameters | Default |
|--|----------|
| Interface maximum number of secure MAC addresses | 1 |
| Security violation action | Shutdown |
| Aging type | Absolute |
| Aging time | 0 |

Configuring Port Security

Enabling or Disabling Port Security Globally

You can enable or disable port security globally on a device. By default, port security is disabled globally.

When you disable port security, all port security configuration on the interface is ineffective. When you disable port security globally, all port security configuration is lost.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters global configuration mode. |
| Step 2 | [no] feature port-security Example: switch(config)# feature port-security | Enables port security globally. The no option disables port security globally. |
| Step 3 | show port-security Example: switch(config)# show port-security | Displays the status of port security. |
| Step 4 | (Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config | Copies the running configuration to the startup configuration. |

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.

You can enable port-security on a port-channel in the following ways:

- Bundle member links into a port-channel by using the **channel-group** command and then enable port-security on the port-channel.
- Create port-channel and configure port security. Configure port security on member links and then bundle member links by using the **channel-group** command. In case of pre-provisioned member links, you can bundle them to the port-channel after the module is online.

Before you begin

You must have enabled port security globally.

If a Layer 2 Ethernet interface is a member of a port-channel interface, you cannot enable or disable port security on the Layer 2 Ethernet interface.

If any member port of a secure Layer 2 port-channel interface has port security enabled, you cannot disable port security for the port-channel interface unless you first remove all secure member ports from the port-channel interface.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: <pre>switch# configure terminal switch(config)#</pre> | Enters global configuration mode. |
| Step 2 | Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> | Enters interface configuration mode for the Ethernet or port-channel interface that you want to configure with port security. |
| Step 3 | switchport Example: <pre>switch(config-if)# switchport</pre> | Configures the interface as a Layer 2 interface. |
| Step 4 | [no] switchport port-security Example: <pre>switch(config-if)# switchport port-security</pre> | Enables port security on the interface. The no option disables port security on the interface. |
| Step 5 | show running-config port-security Example: <pre>switch(config-if)# show running-config port-security</pre> | Displays the port security configuration. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 6 | (Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre> | Copies the running configuration to the startup configuration. |

Enabling or Disabling Sticky MAC Address Learning

You can disable or enable sticky MAC address learning on an interface. If you disable sticky learning, the device returns to dynamic MAC address learning on the interface, which is the default learning method.

By default, sticky MAC address learning is disabled.

Before you begin

You must have enabled port security globally.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: <pre>switch# configure terminal switch(config)#</pre> | Enters global configuration mode. |
| Step 2 | Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> | Enters interface configuration mode for the interface that you want to configure with sticky MAC address learning. |
| Step 3 | switchport Example: <pre>switch(config-if)# switchport</pre> | Configures the interface as a Layer 2 interface. |
| Step 4 | [no] switchport port-security mac-address sticky Example: <pre>switch(config-if)# switchport port-security mac-address sticky</pre> | Enables sticky MAC address learning on the interface. The no option disables sticky MAC address learning. |
| Step 5 | show running-config port-security Example: <pre>switch(config-if)# show running-config port-security</pre> | Displays the port security configuration. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 6 | (Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre> | Copies the running configuration to the startup configuration. |

Adding a Static Secure MAC Address on an Interface

You can add a static secure MAC address on a Layer 2 interface.



Note If the MAC address is a secure MAC address on any interface, you cannot add it as a static secure MAC address to another interface until you remove it from the interface on which it is already a secure MAC address.

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

Before you begin

You must have enabled port security globally.

Verify that the interface maximum has not been reached for secure MAC addresses. If needed, you can remove a secure MAC address or you can change the maximum number of addresses on the interface.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: <pre>switch# configure terminal switch(config)#</pre> | Enters global configuration mode. |
| Step 2 | Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> | Enters interface configuration mode for the interface that you specify. |
| Step 3 | [no] switchport port-security mac-address address [vlan vlan-ID] Example: <pre>switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE</pre> | 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. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 4 | show running-config port-security Example: switch(config-if)# show running-config port-security | Displays the port security configuration. |
| Step 5 | (Optional) copy running-config startup-config Example: switch(config-if)# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Removing a Static Secure MAC Address on an Interface

You can remove a static secure MAC address on a Layer 2 interface.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters global configuration mode. |
| Step 2 | Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: switch(config)# interface ethernet 2/1 switch(config-if)# | Enters interface configuration mode for the interface from which you want to remove a static secure MAC address. |
| Step 3 | no switchport port-security mac-address <i>address</i> Example: switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE | Removes the static secure MAC address from port security on the current interface. |
| Step 4 | show running-config port-security Example: switch(config-if)# show running-config port-security | Displays the port security configuration. |
| Step 5 | (Optional) copy running-config startup-config Example: | Copies the running configuration to the startup configuration. |

| | Command or Action | Purpose |
|--|--|---------|
| | <code>switch(config-if)# copy running-config startup-config</code> | |

Removing a Sticky Secure MAC Address

You can remove a sticky secure MAC addresses, which requires that you temporarily disable sticky address learning on the interface that has the address that you want to remove.

Before you begin

You must have enabled port security globally.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code> | Enters global configuration mode. |
| Step 2 | Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)#</code> | Enters interface configuration mode for the interface from which you want to remove a sticky secure MAC address. |
| Step 3 | no switchport port-security mac-address sticky Example: <code>switch(config-if)# no switchport port-security mac-address sticky</code> | Disables sticky MAC address learning on the interface, which converts any sticky secure MAC addresses on the interface to dynamic secure MAC addresses. |
| Step 4 | clear port-security dynamic address <i>address</i> Example: <code>switch(config-if)# clear port-security dynamic address 0019.D2D0.02GD</code> | Removes the dynamic secure MAC address that you specify. |
| Step 5 | (Optional) show port-security address interface { ethernet <i>slot/port</i> port-channel <i>channel-number</i> } Example: <code>switch(config)# show port-security address</code> | Displays secure MAC addresses. The address that you removed should not appear. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 6 | (Optional) switchport port-security mac-address sticky Example: <pre>switch(config-if)# switchport port-security mac-address sticky</pre> | Enables sticky MAC address learning again on the interface. |

Removing a Dynamic Secure MAC Address

You can remove dynamically learned, secure MAC addresses.

Before you begin

You must have enabled port security globally.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: <pre>switch# configure terminal switch(config)#</pre> | Enters global configuration mode. |
| Step 2 | clear port-security dynamic {interface ethernet slot/port address address} [vlan vlan-ID] Example: <pre>switch(config)# clear port-security dynamic interface ethernet 2/1</pre> | Removes dynamically learned, secure MAC addresses, as specified. If you use the interface keyword, you remove all dynamically learned addresses on the interface that you specify. If you use the address keyword, you remove the single, dynamically learned address that you specify. Use the vlan keyword if you want to further limit the command to removing an address or addresses on a particular VLAN. |
| Step 3 | show port-security address Example: <pre>switch(config)# show port-security address</pre> | Displays secure MAC addresses. |
| Step 4 | (Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre> | Copies the running configuration to the startup configuration. |

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 largest maximum number of addresses that you can configure on an interface is 1025 addresses. The system maximum number of address is 8192.

By default, an interface has a maximum of one secure MAC address. VLANs have no default maximum number of secure MAC addresses.



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

Before you begin

You must have enabled port security globally.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: <pre>switch# configure terminal switch(config)#</pre> | Enters global configuration mode. |
| Step 2 | Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> | Enters interface configuration mode, where <i>slot</i> is the interface that you want to configure with the maximum number of MAC addresses. |
| Step 3 | [no] switchport port-security maximum <i>number</i> [vlan <i>vlan-ID</i>] Example: <pre>switch(config-if)# switchport port-security maximum 425</pre> | Configures the maximum number of MAC addresses that can be learned or statically configured for the current interface. The highest valid <i>number</i> is 1025. 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. |
| Step 4 | show running-config port-security Example: <pre>switch(config-if)# show running-config port-security</pre> | Displays the port security configuration. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 5 | (Optional) copy running-config startup-config Example: <pre>switch(config-if)# copy running-config startup-config</pre> | Copies the running configuration to the startup configuration. |

Configuring an Address Aging Type and Time

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

Absolute aging is the default aging type.

By default, the aging time is 0 minutes, which disables aging.

Before you begin

You must have enabled port security globally.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: <pre>switch# configure terminal switch(config)#</pre> | Enters global configuration mode. |
| Step 2 | Enter one of the following commands: <ul style="list-style-type: none"> interface ethernet <i>slot/port</i> interface port-channel <i>channel-number</i> Example: <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> | Enters interface configuration mode for the interface that you want to configure with the MAC aging type and time. |
| Step 3 | [no] switchport port-security aging type {absolute inactivity} Example: <pre>switch(config-if)# switchport port-security aging type inactivity</pre> | 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. Note F1 series modules do not support the inactivity aging type. |
| Step 4 | [no] switchport port-security aging time minutes Example: <pre>switch(config-if)# switchport port-security aging time 120</pre> | Configures the number of minutes that a dynamically learned MAC address must age before the device drops the address. The maximum valid <i>minutes</i> is 1440. The no option resets the aging time to the default, which is 0 minutes (no aging). |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 5 | show running-config port-security Example: switch(config-if)# show running-config port-security | Displays the port security configuration. |
| Step 6 | (Optional) copy running-config startup-config Example: switch(config-if)# copy running-config startup-config | Copies the running configuration to the startup configuration. |

Configuring a Security Violation Action

You can configure the action that the device takes if a security violation occurs. The violation action is configurable on each interface that you enable with port security.

The default security action is to shut down the port on which the security violation occurs.

Before you begin

You must have enabled port security globally.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters global configuration mode. |
| Step 2 | Enter one of the following commands: <ul style="list-style-type: none"> • interface ethernet <i>slot/port</i> • interface port-channel <i>channel-number</i> Example: switch(config)# interface ethernet 2/1 switch(config-if)# | Enters interface configuration mode for the interface that you want to configure with a security violation action. |
| Step 3 | [no] switchport port-security violation {protect restrict shutdown} Example: switch(config-if)# switchport port-security violation restrict | 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. |
| Step 4 | show running-config port-security Example: | Displays the port security configuration. |

| | Command or Action | Purpose |
|---------------|---|--|
| | <code>switch(config-if)# show running-config port-security</code> | |
| Step 5 | (Optional) copy running-config startup-config Example: <code>switch(config-if)# copy running-config startup-config</code> | Copies the running configuration to the startup configuration. |

Verifying the Port Security Configuration

To display the port security configuration information, perform one of the following tasks. For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

| Command | Purpose |
|--|--|
| show running-config port-security | Displays the port security configuration. |
| show port-security | Displays the port security status of the device. |
| show port-security interface | Displays the port security status of a specific interface. |
| show port-security address | Displays secure MAC addresses. |

Displaying Secure MAC Addresses

Use the **show port-security address** command to display secure MAC addresses. For detailed information about the fields in the output from this command, see the

Configuration Example for Port Security

The following example shows a port security configuration for the Ethernet 2/1 interface with VLAN and interface maximums for secure addresses. In this example, the interface is a trunk port. Additionally, the violation action is set to Restrict.

```
feature port-security
interface Ethernet 2/1
  switchport
  switchport port-security
  switchport port-security maximum 10
  switchport port-security maximum 7 vlan 10
  switchport port-security maximum 3 vlan 20
  switchport port-security violation restrict
```

Configuration Example of Port Security in a vPC Domain

The following example shows how to enable and configure port security on vPC peers in a vPC domain. The first switch is the primary vPC peer and the second switch is the secondary vPC peer. It is assumed that domain 103 has already been created.

```
primary_switch(config)# feature port-security
primary_switch(config-if)# int e1/1
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# int e103/1/1
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# copy running-config startup-config
```

Additional References for Port Security

Related Documents

Standards

| Standards | Title |
|---|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

MIBs

Cisco NX-OS provides read-only SNMP support for port security.

| MIBs | MIBs Link |
|---|---|
| <ul style="list-style-type: none"> CISCO-PORT-SECURITY-MIB <p>Note Traps are supported for notification of secure MAC address violations.</p> | <p>To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p> |

