CHAPTER 13

Configuring Port Security

This chapter describes how to configure port security on NX-OS devices.

This chapter includes the following sections:

Information About Port Security

Port security allows you to configure Layer 2 interfaces that 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.

This section includes the following topics:

Secure MAC Address Learning

The process of securing a MAC address is called learning. The number of addresses that can be learned is restricted, as described in the "Secure MAC Address Maximums" section on page 13-3. For each interface that you enable port security on, the device can learn addresses by the static, dynamic, or sticky methods.

Static Method

The static learning method allows you to manually add or remove secure MAC addresses to the configuration of an interface.

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. For more information, see the "Removing a Static or a Sticky Secure MAC Address on an Interface" section on page 13-12.
- You configure the interface to act as a Layer 3 interface. For more information, see the "Port Type Changes" section on page 13-5.

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 ages dynamic addresses and drops them once the age limit is reached, as described in the "Dynamic Address Aging" section on page 13-3.

Dynamic addresses do not persist through a device restart or through restarting the interface.

To remove a specific address learned by the dynamic method or to remove all addresses learned by the dynamic method on a specific interface, see the "Removing a Dynamic Secure MAC Address" section on page 13-13.

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 non-volatile 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.

The device does not age sticky secure MAC addresses.

To remove a specific address learned by the sticky method, see the "Removing a Static or a Sticky Secure MAC Address on an Interface" section on page 13-12.

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 0 to 1440 minutes, where 0 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.

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.

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 address are permitted on an interface:

- Device 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 secure MAC addresses for each interface protected by port security. The default interface maximum is one address. Interface maximums cannot exceed the device maximum.
- VLAN maximum—You can configure the maximum number of 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.

  For an example of how VLAN and interface maximums interact, see the "Security Violations and Actions" section on page 13-4.

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. To remove dynamically learned addresses, see the "Removing a Dynamic Secure MAC Address" section on page 13-13. To remove addresses learned by the sticky or static methods, see the "Removing a Static or a Sticky Secure MAC Address on an Interface" section on page 13-12.

Security Violations and Actions

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

- Ingress traffic arrives at an interface from a nonsecure MAC address and learning the address would exceed the applicable maximum number of secure MAC addresses.

  When an interface has both a VLAN maximum and an interface maximum configured, a violation occurs when either maximum is exceeded. For example, consider the following on a single interface configured with port security:

  - VLAN 1 has a maximum of 5 addresses
  - The interface has a maximum of 10 addresses

  The device detects a violation when any of the following occurs:

  - The device has learned five addresses for VLAN 1 and inbound traffic from a sixth address arrives at the interface in VLAN 1.
  - The device has learned 10 addresses on the interface and inbound traffic from an 11th address arrives at the interface.
- Ingress traffic from a secure MAC address arrives at a different interface in the same VLAN as the interface on which the address is secured.

Note After a secure MAC address is configured or learned on one secure port, the sequence of events that occurs when port security detects that secure MAC address on a different port in the same VLAN is known as a MAC move violation.

When a security violation occurs, the device takes the action specified by the port security configuration of the applicable interface. The possible actions 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.
- Restrict—Drops ingress traffic from any nonsecure MAC addresses. The device keeps a count of the number of dropped packets.
- 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.

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.

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 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 Port Channels—Port security is not supported on Ethernet port channels.

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 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.
- 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.

802.1X and Port Security

You can configure port security and 802.1X on the same interfaces. Port security secures the MAC addresses that 802.1X authenticates. 802.1X processes packets before port security processes them, so when you enable both on an interface, 802.1X is already preventing inbound traffic on the interface from unknown MAC addresses.

When you enable 802.1X and port security on the same interface, port security continues to learn MAC addresses by the sticky or dynamic method, as configured. Additionally, depending on whether you enable 802.1X in single-host mode or multiple-host mode, one of the following occurs:

- Single host mode—Port security learns the MAC address of the authenticated host.
- Multiple host mode—Port security drops any MAC addresses learned for this interface by the dynamic method and learns the MAC address of the first host authenticated by 802.1X.

If a MAC address that 802.1X passes to port security would violate the applicable maximum number of secure MAC addresses, the device sends an authentication failure message to the host.

The device treats MAC addresses authenticated by 802.1X as though they were learned by the dynamic method, even if port security previously learned the address by the sticky or static methods. If you attempt to delete a secure MAC address that has been authenticated by 802.1X, the address remains secure.

If the MAC address of an authenticated host is secured by the sticky or static method, the device treats the address as if it were learned by the dynamic method, and you cannot delete the MAC address manually.

Port security integrates with 802.1X to reauthenticate hosts when the authenticated and secure MAC address of the host reaches its port security age limit. The device behaves differently depending upon the type of aging, as follows:

- Absolute—Port security notifies 802.1X and the device attempts to reauthenticate the host. The result of reauthentication determines whether the address remains secure. If reauthentication succeeds, the device restarts the aging timer on the secure address; otherwise, the device drops the address from the list of secure addressees for the interface.
- Inactivity—Port security drops the secure address from the list of secure addresses for the interface and notifies 802.1X. The device attempts to reauthenticate the host. If reauthentication succeeds, port security secures the address again.

Virtualization Support

Port security supports VDCs as follows:

- Port security is local to each VDC. You enable and configure port security on a per-VDC basis.
- Each VDC maintains secure MAC addresses separately.
- The device cannot issue a security violation when a secured MAC address in one VDC is seen on a protected interface in another VDC.

Licensing Requirements for Port Security

The following table shows the licensing requirements for this feature:

Product	License Requirement
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. For a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0*.

Prerequisites for Port Security

Port security has the following prerequisites:

- You must globally enable port security for the device that you want to protect with port security.

Guidelines and Limitations

When configuring port security, follow these guidelines:

- Port security does not support Ethernet port-channel interfaces or switched port analyzer (SPAN) destination ports.
- Port security does not depend upon other features.
- Port security can work with 802.1X, as described in the "802.1X and Port Security" section on page 13-5.

Configuring Port Security

This section includes the following topics:

Enabling or Disabling Port Security Globally

You can enable or disable port security globally on a device.

When you disable port security globally, all port security configuration is lost, including any statically configured secure MAC addresses and all dynamic or sticky secured MAC addresses.

BEFORE YOU BEGIN

By default, port security is disabled.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **[no] feature port-security**
3. **show port-security**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t 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	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) 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. For more information about dynamic learning of MAC addresses, see the "Secure MAC Address Learning" section on page 13-2.

Note You cannot enable port security on a routed interface.

BEFORE YOU BEGIN

By default, port security is disabled on all interfaces.

Enabling port security on an interface also enables dynamic MAC address learning. If you want to enable sticky MAC address learning, you must also complete the steps in the "Enabling or Disabling Sticky MAC Address Learning" section on page 13-9.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that port security is enabled. To verify the configuration, see the "Verifying the Port Security Configuration" section on page 13-17. To enable port security, see the "Enabling or Disabling Port Security Globally" section on page 13-7.

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **switchport**
4. [no] **switchport port-security**
5. **show running-config port-security**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode for the interface that you want to configure with port security.
Step 3	**switchport** **Example:** switch(config-if)# switchport	Configures the interface as a Layer 2 interface.
Step 4	[**no**] **switchport port-security** **Example:** switch(config-if)# switchport port-security	Enables port security on the interface. The **no** option disables port security on the interface.
Step 5	**show running-config port-security** **Example:** switch(config-if)# show running-config port-security	Displays the port security configuration.
Step 6	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	(Optional) 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.

BEFORE YOU BEGIN

By default, sticky MAC address learning is disabled.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that port security is enabled globally and on the interface that you are configuring. To verify the configuration, see the "Verifying the Port Security Configuration" section on page 13-17. To enable port security globally, see the "Enabling or Disabling Port Security Globally" section on page 13-7. To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 13-8.

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **switchport**
4. **[no] switchport port-security mac-address sticky**
5. **show running-config port-security**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode for the interface that you want to configure with sticky MAC address learning.
Step 3	**switchport** **Example:** switch(config-if)# switchport	Configures the interface as a Layer 2 interface.
Step 4	[**no**] **switchport port-security mac-address sticky** **Example:** switch(config-if)# switchport port-security mac-address sticky	Enables sticky MAC address learning on the interface. The **no** option disables sticky MAC address learning.
Step 5	**show running-config port-security** **Example:** switch(config-if)# show running-config port-security	Displays the port security configuration.
Step 6	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	(Optional) 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.

BEFORE YOU BEGIN

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

Determine if the interface maximum has been reached for secure MAC addresses (use the **show port-security** command). If needed, you can remove a secure MAC address (see the "Removing a Static or a Sticky Secure MAC Address on an Interface" section on page 13-12 or the "Removing a Dynamic Secure MAC Address" section on page 13-13) or you can change the maximum number of addresses on the interface (see the "Configuring a Maximum Number of MAC Addresses" section on page 13-13).

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that port security is enabled both globally and on the interface. To verify the configuration, see the "Verifying the Port Security Configuration" section on page 13-17. To enable port security globally, see the "Enabling or Disabling Port Security Globally" section on page 13-7. To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 13-8.

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. [**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode for the interface that you specify.
Step 3	[**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*] **Example:** switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE	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	**show running-config port-security** **Example:** switch(config-if)# show running-config port-security	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

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

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

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that port security is enabled. To verify the configuration, see the "Verifying the Port Security Configuration" section on page 13-17. To enable port security globally, see the "Enabling or Disabling Port Security Globally" section on page 13-7. To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 13-8.

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. **no switchport port-security mac-address** *address* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode for the interface from which you want to remove a secure static or sticky MAC address.
Step 3	**no switchport port-security mac-address** *address* **Example:** switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE	Removes the 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	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Removing a Dynamic Secure MAC Address

You can remove dynamically learned, secure MAC addresses.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

SUMMARY STEPS

1. **config t**
2. **clear port-security dynamic** {**interface ethernet** *slot/port* | **address** *address*} [**vlan** *vlan-ID*]
3. **show port-security address**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**clear port-security dynamic** {**interface ethernet** *slot/port* | **address** *address*} [**vlan** *vlan-ID*] **Example:** switch(config)# clear port-security dynamic interface ethernet 2/1	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:** switch(config)# show port-security address	Displays secure MAC addresses.

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 is 4096 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 reduce the number of addresses learned by the sticky or static methods, see the "Removing a Static or a Sticky Secure MAC Address on an Interface" section on page 13-12. To remove all addresses learned by the dynamic method, use the **shutdown** and **no shutdown** commands to restart the interface.

BEFORE YOU BEGIN

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

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that port security is enabled. To verify the configuration, see the "Verifying the Port Security Configuration" section on page 13-17. To enable port security, see the "Enabling or Disabling Port Security Globally" section on page 13-7.

SUMMARY STEPS

1. **config t**
2. **interface** *type slot*
3. [**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*]
4. **show running-config port-security**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**interface** *type slot* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode, where *slot* is the interface that you want to configure with the maximum number of MAC addresses.
Step 3	[**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*] **Example:** switch(config-if)# switchport port-security maximum 425	Configures the maximum number of MAC addresses that can be learned or statically configured for the current interface. The highest valid *number* is 4096. 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.

	Command	Purpose
Step 4	**show running-config port-security** **Example:** `switch(config-if)# show running-config port-security`	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	(Optional) 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.

BEFORE YOU BEGIN

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

Absolute aging is the default aging type.

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that port security is enabled. To verify the configuration, see the "Verifying the Port Security Configuration" section on page 13-17. To enable port security, see the "Enabling or Disabling Port Security Globally" section on page 13-7.

SUMMARY STEPS

1. **config t**
2. **interface** *type slot*
3. [**no**] **switchport port-security aging type** {**absolute** | **inactivity**}
4. [**no**] **switchport port-security aging time** *minutes*
5. **show running-config port-security**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *type slot*
	
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Enters interface configuration mode, where *slot* is the interface that you want to configure with MAC aging type and time.

	Command	Purpose
Step 3	[no] **switchport port-security aging type** {**absolute** | **inactivity**} **Example:** switch(config-if)# switchport port-security aging type 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	[no] **switchport port-security aging time** *minutes* **Example:** switch(config-if)# switchport port-security aging time 120	Configures the number of minutes that a dynamically learned MAC address must age before the device drops the address. The maximum valid *minutes* is 1440. The **no** option resets the aging time to the default, which is 0 minutes (no aging).
Step 5	**show running-config port-security** **Example:** switch(config-if)# show running-config port-security	Displays the port security configuration.
Step 6	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	(Optional) 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.

BEFORE YOU BEGIN

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

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that port security is enabled. To verify the configuration, see the "Verifying the Port Security Configuration" section on page 13-17. To enable port security, see the "Enabling or Disabling Port Security Globally" section on page 13-7.

SUMMARY STEPS

1. **config t**
2. **interface** *type slot/port*
3. [**no**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**}
4. **show running-config port-security**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** switch(config)# interface ethernet 2/1 switch(config-if)#	Enters interface configuration mode, where *slot* is the interface for which you want to configure the 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:** switch(config-if)# show running-config port-security	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** switch(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Verifying the Port Security Configuration

To display the port security configuration information, use the following commands:

Command	Purpose
show running-config port-security	Displays the port security configuration
show port-security	Displays the port security status.

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

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 *Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*.

Example Configuration 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
```

Default Settings

Table 13-1 lists the default settings for port security parameters.

Table 13-1 Default Port Security Parameters

Parameters	Default
Port security enablement globally	Disabled
Port security enablement per interface	Disabled
MAC address learning method	Dynamic
Interface maximum number of secure MAC addresses	1
Security violation action	Shutdown

Additional References

For additional information related to implementing port security, see the following sections:

- Related Documents, page 13-18
- Standards, page 13-19
- MIBs, page 13-19

Related Documents

Related Topic	Document Title
Layer 2 switching	*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.0*
Port security commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0*

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

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

MIBs	MIBs Link
• CISCO-PORT-SECURITY-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/nx-os/mibs