CHAPTER 11

Configuring Port Security

This chapter describes how to configure port security and includes the following sections:

Information About Port Security

Port security lets you configure Layer 2 interfaces permitting 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.

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 11-3. Address learning can be accomplished using the following methods on any interface where port security is enabled:

- Dynamic Method, page 11-2 (the default method)
- Sticky Method, page 11-2

Static Method

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

A static secure MAC address entry remains in the configuration of an interface until you explicitly remove it. For more information, see the "Removing a Static or a Sticky Secure MAC Address from an Interface" section on page 11-10.

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.

Dynamic addresses are aged and dropped once the age limit is reached, as described in the "Dynamic Address Aging" section on page 11-2.

Dynamic addresses do not persist through restarts.

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 11-11.

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 copying the running-configuration to the startup-configuration, **copy run start**.

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.

To remove a specific address learned by the sticky method, see the "Removing a Static or a Sticky Secure MAC Address from an Interface" section on page 11-10.

Dynamic Address Aging

MAC addresses 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 address age:

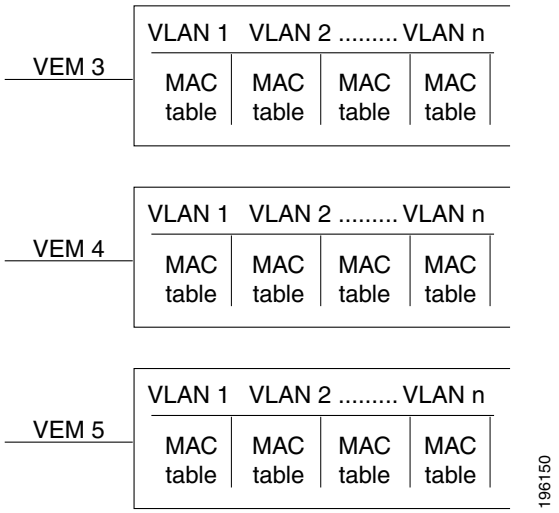
- Inactivity—The length of time after the device last received a packet from the address on the applicable interface.
- Absolute—The length of time after the device learned the address. This is the default aging method; however, the default aging time is 0 minutes, which disables aging.

Secure MAC Address Maximums

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

Figure 11-1 shows that each VLAN in a VEM has a forwarding table that can store a maximum number of secure MAC addresses. For current MAC address maximums, see Security Configuration Limits, page 17-1.

Figure 11-1 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.

Tip To make use of 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 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 11-4.

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 11-11. To remove addresses learned by the sticky or static methods, see the "Removing a Static or a Sticky Secure MAC Address from an Interface" section on page 11-10.

Security Violations and Actions

Port security triggers a security violation when either of the following occurs:

- 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

  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.
- 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 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.

Example:

```
n1000v(config)# errdisable recovery cause psecure-violation
n1000v(config)# copy running-config startup-config (Optional)
```

- 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 action is applied on the interface that received the traffic. A MAC Move Violation is triggered on the port seeing the MAC which is already secured on another interface.

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 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 an access port to a trunk port on a Layer 2 interface configured with port security, all secure addresses learned by the dynamic method are dropped. The device to the native trunk VLAN moves the addresses learned by the static or sticky method.

Result of Changing a Trunk Port to an Access Port

When you change a trunk port to an access port on a Layer 2 interface configured with port security, all secure addresses learned by the dynamic method are dropped. All configured and sticky MAC addresses are dropped if they are not on the native trunk VLAN and do not match the access VLAN configured for the access port they are moving to.

Guidelines and Limitations

When configuring port security, follow these guidelines:

- Port security is not supported on the following:
  - Ethernet interfaces
  - Ethernet port-channel interfaces

  - Switched port analyzer (SPAN) destination ports
- The port security feature cannot be applied for the Control, Management, and AIPC interfaces of the VSM.
- Port security does not depend upon other features.
- Port security does not support 802.1X.
- Port Security cannot be configured on interfaces with existing static MACs.
- Port Security cannot be enabled on interfaces whose VLANs have an existing static MAC even if it is programmed on a different interface.

Default Settings

Table 11-1 lists the default settings for port security parameters.

Table 11-1 Default Port Security Parameters

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

Configuring Port Security

This section includes the following topics:

Enabling or Disabling Port Security on a Layer 2 Interface

Use this procedure to 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 11-1.

Note You cannot enable port security on a routed interface.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- 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 11-8.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.

	Command	Purpose
Step 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	Places you into Interface Configuration mode for the specified interface.
Step 3	[**no**] **switchport port-security** **Example:** n1000v(config-if)# switchport port-security	Enables port security on the interface. Using the **no** option disables port security on the interface.
Step 4	**show running-config port-security** **Example:** n1000v(config-if)# show running-config port-security	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Enabling or Disabling Sticky MAC Address Learning

Use this procedure to disable or enable sticky MAC address learning on an interface.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Dynamic MAC address learning is the default on an interface.
- By default, sticky MAC address learning is disabled.
- Make sure that port security is enabled on the interface that you are configuring.
  - To verify the configuration, see the "Verifying the Port Security Configuration" section on page 11-18.
  - To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 11-7.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	Places you into Interface Configuration mode for the specified interface.
Step 3	[**no**] **switchport port-security mac-address sticky** **Example:** n1000v(config-if)# 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	**show running-config port-security** **Example:** n1000v(config-if)# show running-config port-security	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(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

Use this procedure to add a static secure MAC address on a Layer 2 interface.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- 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 one of the following:
  - "Removing a Static or a Sticky Secure MAC Address from an Interface" section on page 11-10
  - "Removing a Dynamic Secure MAC Address" section on page 11-11)
  - "Configuring a Maximum Number of MAC Addresses" section on page 11-12).
- Make sure that port security is enabled on the interface that you are configuring.
  - To verify the configuration, see the "Verifying the Port Security Configuration" section on page 11-18.

– To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 11-7.

SUMMARY STEPS

1. **config t**
2. **interface** *type number*
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:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**interface** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(config-if)#`
		Places you into Interface Configuration mode for the specified interface.

Step 3	[**no**] **switchport port-security mac-address** *address* [**vlan** *vlan-ID*] **Example:** `n1000v(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:** `n1000v(config-if)# show running-config port-security`	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** `n1000v(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 from an Interface

Use this procedure to remove a static or a sticky secure MAC address from a Layer 2 interface.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Make sure that port security is enabled on the interface that you are configuring.

- To verify the configuration, see the "Verifying the Port Security Configuration" section on page 11-18.
- To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 11-7.

SUMMARY STEPS

1. **config t**
2. **interface** *type number*
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:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**interface** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(config-if)#`
		Places you into Interface Configuration mode for the specified interface.

Step 3	**no switchport port-security mac-address** *address* **Example:** `n1000v(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:** `n1000v(config-if)# show running-config port-security`	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-if)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Removing a Dynamic Secure MAC Address

Use this procedure to remove a dynamically learned, secure MAC address.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**clear port-security dynamic** {**interface vethernet** *number* | **address** *address*} [**vlan** *vlan-ID*] **Example:** `n1000v(config)# clear port-security dynamic interface vethernet 36`	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:** `n1000v(config)# show port-security address`	Displays secure MAC addresses.

Configuring a Maximum Number of MAC Addresses

Use this procedure to 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 command is rejected.

To reduce the number of addresses learned by the sticky or static methods, see the "Removing a Static or a Sticky Secure MAC Address from an Interface" section on page 11-10.

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

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- The Secure MACs share the L2 Forwarding Table (L2FT). The forwarding table for each VLAN can hold up to 1024 entries.
- By default, an interface has a maximum of one secure MAC address.
- VLANs have no default maximum number of secure MAC addresses.
- Make sure that port security is enabled on the interface that you are configuring.
  - To verify the configuration, see the "Verifying the Port Security Configuration" section on page 11-18.
  - To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 11-7.

SUMMARY STEPS

1. **config t**
2. **interface** ***type*** *number*
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:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**interface** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(config-if)#`
		Places you into Interface Configuration mode for the specified interface.

Step 3	[**no**] **switchport port-security maximum** *number* [**vlan** *vlan-ID*] **Example:** `n1000v(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:** `n1000v(config-if)# show running-config port-security`	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-if)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring an Address Aging Type and Time

Use this procedure to 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.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- By default, the aging time is 0 minutes, which disables aging.
- Absolute aging is the default aging type.
- Make sure that port security is enabled on the interface that you are configuring.
  - To verify the configuration, see the "Verifying the Port Security Configuration" section on page 11-18.
  - To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 11-7.

SUMMARY STEPS

1. **config t**
2. **interface** ***type*** *number*
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:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	Places you into Interface Configuration mode for the specified interface.
Step 3	[**no**] **switchport port-security aging type** {**absolute** | **inactivity**} **Example:** n1000v(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:** n1000v(config-if)# switchport port-security aging time 120	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	**show running-config port-security** **Example:** n1000v(config-if)# show running-config port-security	Displays the port security configuration.
Step 6	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring a Security Violation Action

Use this procedure to configure how an interface responds to a security violation.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- The default security action is to shut down the port on which the security violation occurs.
- 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.

  For more information, see the "Security Violations and Actions" section on page 11-4.

- Make sure that port security is enabled on the interface that you are configuring.
  - To verify the configuration, see the "Verifying the Port Security Configuration" section on page 11-18.
  - To enable port security on the interface, see the "Enabling or Disabling Port Security on a Layer 2 Interface" section on page 11-7.

SUMMARY STEPS

1. **config t**
2. **interface** *type number*
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:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**interface** *type number* **Example:** n1000v(config)# interface vethernet 36 n1000v(config-if)#	Places you into Interface Configuration mode for the specified interface.
Step 3	[**no**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**} **Example:** n1000v(config-if)# switchport port-security violation protect	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. • **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 increments the SecurityViolation counter. • **shutdown**: (the default) Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

	Command	Purpose
Step 4	**show running-config port-security** **Example:** `n1000v(config-if)# show running-config port-security`	Displays the port security configuration.
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-if)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Recovering Ports Disabled for Port Security Violations

Use this procedure to automatically recover an interface disabled for port security violations.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- To recover an interface manually from the error-disabled state, you must enter the **shutdown** command and then the **no shutdown** command .
- For more information, see the "Security Violations and Actions" section on page 11-4.

SUMMARY STEPS

1. **config t**
2. **interface** *type number*
3. **errdisable recovery cause psecure-violation**
4. **errdisable recovery interval** *seconds*
5. **show interface** *type number*

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**interface** *type number*
	
	Example:
	`n1000v(config)# interface vethernet 36`
	`n1000v(config-if)#`
		Places you into Interface Configuration mode for the specified interface.

	Command	Purpose
Step 3	**errdisable recovery cause psecure-violation** **Example:** `n1000v(config-if)# errdisable recovery cause psecure-violation`	Enables timed automatic recovery of the specified port that is disabled for port security violation.
Step 4	**errdisable recovery interval** *seconds* **Example:** `n1000v(config-if)# errdisable recovery interval 30`	Configures a timer recovery interval in seconds from 30 to 65535 seconds.
Step 5	**show interface** *type number* **Example:** `n1000v(config-if)# show running-config port-security`	Displays theinterface state for verification.

Verifying the Port Security Configuration

Use the following commands to display the port security configuration information:

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 1000V Command Reference, Release 4.2(1)SV1(5.1)*.

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 1000V Command Reference, Release 4.2(1)SV1(5.1)*.

Example Configuration for Port Security

The following example shows a port security configuration for vEthernet 36 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 Protect.

```
interface vethernet 36
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 protect
```

Additional References

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

- Related Documents, page 11-19
- Standards, page 11-19

Related Documents

Related Topic	Document Title
Layer 2 switching	*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV1(5.1)*
Port security commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*

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.	—

Feature History for Port Security

This section provides the port security feature release history.

Feature Name	Releases	Feature Information
Port Security	4.0(4)SV1(1)	This feature was introduced.