Configuring Port Security

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

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

Information About Port Security

Port security allows you to configure Layer 2 physical interfaces and Layer 2 port-channel 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.

Note Unless otherwise specified, the term *interface* refers to both physical interfaces and port-channel interfaces; 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.

Related Topics

- Secure MAC Address Maximums, page 3

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.

Related Topics

- Removing a Static Secure MAC Address on an Interface, page 14
- Port Type Changes, page 7

Dynamic Method

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

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

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

- You configure the interface to act as a Layer 3 interface.

Related Topics

- Dynamic Address Aging, page 3
- Removing a Dynamic or Sticky Secure MAC Address, page 15

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 in the configuration of an interface until one of the following events occurs:

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

Related Topics

- Removing a Dynamic or Sticky Secure MAC Address, page 15

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 addresses 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 1025 secure MAC addresses.
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 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.

Related Topics

- Security Violations and Actions, page 4
- Configuring a Maximum Number of MAC Addresses, page 16
- Removing a Dynamic or Sticky Secure MAC Address, page 15
- Removing a Static Secure MAC Address on an Interface, page 14

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 increments the security violation counter for the interface and takes the action specified by the port security configuration of the 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.
Restrict	Drops ingress traffic from any nonsecure MAC addresses. Address learning continues until 100 security violations have occurred on the interface. Traffic from addresses learned after the first security violation is dropped. After 100 security violations occur, the device disables learning on the interface and drops all ingress traffic from nonsecure MAC addresses. In addition, the device generates an SNMP notification for each security violation.
Protect	Prevents further violations from occurring. The address that triggered the security violation is learned but any traffic from the address is dropped. Further address learning stops.

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	You can configure port security on Layer 2 Ethernet port channels in either access mode or trunk mode.
Virtual port channels	Port security is not supported on virtual port channels.

Port Security and Port-Channel Interfaces

Port security is supported on Layer 2 port-channel interfaces. Port security operates on port-channel interfaces in the same manner as on physical interfaces, except as described in this section.

General guidelines

Port security on a port-channel interface operates in either access mode or trunk mode. In trunk mode, the MAC address restrictions enforced by port security apply to all member ports on a per-VLAN basis.

Enabling port security on a port-channel interface does not affect port-channel load balancing.

Port security does not apply to port-channel control traffic passing through the port-channel interface. Port security allows port-channel control packets to pass without causing security violations. Port-channel control traffic includes the following protocols:

- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- Inter-Switch Link (ISL)
- IEEE 802.1Q

Configuring secure member ports

The port security configuration of a port-channel interface has no effect on the port security configuration of member ports.

Adding a member port

If you add a secure interface as a member port of a port-channel interface, the device discards all dynamic secure addresses learned on the member port but retains all other port-security configuration of the member port in the running configuration. Sticky and static secure MAC addresses learned on the secure member port are also stored in the running configuration rather than NVRAM.

If port security is enabled on the member port and not enabled on the port-channel interface, the device warns you when you attempt to add the member port to the port-channel interface.

While a port is a member of a port-channel interface, you cannot configure port security on the member port. To do so, you must first remove the member port from the port-channel interface.

Removing a member port

If you remove a member port from a port-channel interface, the device restores the port security configuration of the member port. Static and sticky secure MAC addresses that were learned on the port before you added it to the port-channel interface are restored to NVRAM and removed from the running configuration.

Note To ensure that all ports are secure as needed after you remove a port-channel interface, we recommend that you closely inspect the port-security configuration of all member ports.

Removing a port-channel interface

If you remove a secure port-channel interface, the following occurs:

- The device discards all secure MAC addresses learned for the port-channel interface, including static and sticky secure MAC addresses learned on the port-channel interface.
- The device restores the port-security configuration of each member port. The static and sticky secure MAC addresses that were learned on member ports before you added them to the port-channel interface are restored to NVRAM and removed from the running configuration. If a member port did not have port security enabled prior to joining the port-channel interface, port security is not enabled on the member port after the port-channel interface is removed.

Note To ensure that all ports are secure as needed after you remove a port-channel interface, we recommend that you closely inspect the port-security configuration of all member ports.

Disabling port security

If port security is enabled on any member port, the device does not allow you to disable port security on the port-channel interface. To do so, remove all secure member ports from the port-channel interface first. After disabling port security on a member port, you can add it to the port-channel interface again, as needed.

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 for Port Security

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
DCNM	Port security requires a LAN Enterprise license. For a complete explanation of the DCNM licensing scheme and how to obtain and apply licenses, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.2*
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. For a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2*.

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 for Port Security

When configuring port security, follow these guidelines:

- Port security supports PVLANs. If a device learns a secure MAC address learned from traffic on the secondary VLAN of a PVLAN, it secures the MAC address on the primary VLAN.
- Port security does not support switched port analyzer (SPAN) destination ports.
- Port security does not depend upon other features.
- Port security operates with 802.1X on Layer 2 Ethernet interfaces.
- For each device that you use DCNM to configure port security, ensure that you configure the logging level for port security to 5 (Notifications) or a higher level. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

```
switch(config)# logging level port-security 5
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

For more information about Cisco NX-OS system-message logging requirements, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.2*.

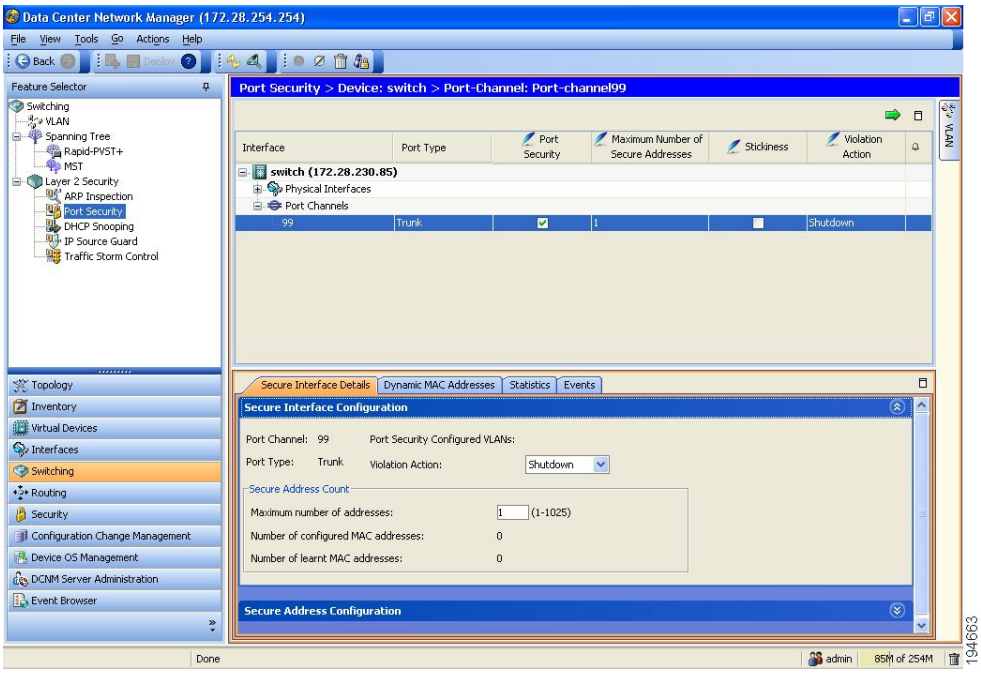
Related Topics

- 802.1X and Port Security, page 8

Configuring Port Security

This figure shows the Port Security content pane.

Figure 1: Port Security Content Pane



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 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

Ensure that you configure the logging level for port security to 5 (Informational) or a higher level on the Cisco NX-OS device. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

```
switch(config)# logging level port-security 5
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

For more information about Cisco NX-OS system-message logging requirements, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.2*.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 From the Summary pane, click the device on which you want to enable or disable port security.

Step 3 From the menu bar, do one of the following:

- If you want to enable port security globally on the device, choose **Actions ➤ Enable Port Security Service**.
- If you want to disable port security globally on the device, choose **Actions ➤ Disable Port Security Service**.

When port security is enabled, the Stop Learning check box appears on the Global Settings tab in the Details pane.

When port security is disabled, the Port Security is disabled on device message appears on the Global Settings tab in the Details pane.

You do not need to save your changes.

Enabling or Disabling Port Security on a Layer 2 Interface

You can enable or disable port security on a Layer 2 physical interface or Layer 2 port-channel interface. By default, port security is disabled on all interfaces.

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

Note You cannot enable port security on a routed interface.

Before You Begin

Port security must be enabled globally.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 If the interface that you want to configure does not appear, do the following:

a) From the menu bar, choose **Actions ➤ Add Interface**.
Below the selected interface type, a new row contains a drop-down list in the Interface column.

b) In the Interface column, from the drop-down list, choose the interface on which you want to enable port security.

The interface name appears in the new row of the Summary pane.

Step 4 Click the interface and then do one of the following:

- To enable port security on the selected interface, in the Port Security column, check the check box.
- To disable port security on the selected interface, in the Port Security column, uncheck the check box.

DCNM enables or disables port security on the interface, as specified. You do not need to save your changes.

Related Topics

- Secure MAC Address Learning, page 2
- Enabling or Disabling Sticky MAC Address Learning, page 12

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

Port security must be enabled globally.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 If the interface that you want to configure does not appear, do the following:

a) From the menu bar, choose **Actions ➤ Add Interface**.
Below the selected interface type, a new row contains a drop-down list in the Interface column.

b) In the Interface column, from the drop-down list, choose the interface on which you want to enable port security.

The interface name appears in the new row of the Summary pane.

Step 4 Click the interface on which you want to enable or disable sticky MAC address learning.

Step 5 Do one of the following:

- To enable sticky MAC address learning on the selected interface, in the Stickiness column, check the check box.
- To disable sticky MAC address learning on the selected interface, in the Stickiness column, uncheck the check box.

Step 6 From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.

Adding a Static Secure MAC Address on an Interface

You can add a static secure MAC address on a Layer 2 interface. If the interface is in trunk port mode, you must assign the new static secure MAC address to a VLAN.

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

Before You Begin

Port security must be enabled globally.

Display the secure MAC addresses on the interface and determine if the interface maximum for secure MAC addresses has been reached. If needed, you can remove a secure MAC address or you can change the maximum number of addresses on the interface.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 If the interface that you want to configure does not appear, do the following:

a) From the menu bar, choose **Actions ➤ Add Interface**.
Below the selected interface type, a new row contains a drop-down list in the Interface column.

b) In the Interface column, from the drop-down list, choose the interface on which you want to enable port security.

The interface name appears in the new row of the Summary pane.

Step 4 Click the interface on which you want to configure an address.

Step 5 From the Details pane, click the **Secure Interface Details** tab.

Step 6 Expand the **Secure Address Configuration** section, if necessary.
A table of secure MAC addresses appears in the Secure Address Configuration section. If the interface that you selected is in trunk port mode, the table is organized by VLAN ID.

Step 7 If the interface is in trunk port mode and the VLAN for the new secure address does not appear, do the following:

a) Right-click either on an existing VLAN entry or on a blank row.

b) Choose **Add VLAN**.
A new row appears, with a drop-down list in the VLAN ID column.

c) From the drop-down list, choose the VLAN ID that you need to associate the secure address with.

Step 8 Under the Host MAC Address heading, right-click on a blank area and choose **Add Host**.
A new row appears under the Host MAC Address heading.

Step 9 Double-click on the new row, type the new static secure MAC address, and press **Enter**.
Valid entries are dotted hexadecimal MAC addresses.

DCNM configures the static secure MAC address on the interface. You do not need to save your changes.

Related Topics

- Configuring a Maximum Number of MAC Addresses, page 16
- Removing a Dynamic or Sticky Secure MAC Address, page 15
- Removing a Static Secure MAC Address on an Interface, page 14

Removing a Static Secure MAC Address on an Interface

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

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 Click the interface from which you want to delete an address.

Step 4 From the Details pane, click the **Secure Interface Details** tab.

Step 5 If necessary, expand the **Secure Address Configuration** section.
A table of secure MAC addresses appears in the Secure Address Configuration section. If the interface that you selected is in trunk port mode, the table is organized by VLAN ID.

Step 6 If the interface is in trunk port mode, expand the VLAN that you need to remove the secure address from.
Secure MAC addresses associated with the selected VLAN appear in the table below the Host MAC Address heading.

Step 7 Right-click the address that you need to remove and choose **Delete Host**.
A confirmation warning appears.

Step 8 Click **Yes**.
DCNM removes the static secure MAC address from the interface configuration. If the interface is in trunk port mode and you removed the last static secure MAC address from a VLAN, that VLAN no longer appears in the Secure Address Configuration section.

You do not need to save your changes.

Removing a Dynamic or Sticky Secure MAC Address

You can remove dynamically learned, secure MAC addresses, including sticky secure MAC addresses.

Before You Begin

Port security must be enabled globally.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 Click the interface from which you want to delete a dynamic or sticky secure MAC address.

Step 4 From the Details pane, click the **Dynamic MAC Addresses** tab.
A table of dynamic secure MAC addresses, organized by VLAN ID, appears.

Step 5 If necessary, expand the VLAN that you need to remove the secure address from.

Secure MAC addresses associated with the selected VLAN appear in the table below the Host MAC Address heading.

Step 6 Right-click the address that you need to remove and choose **Clear MAC Address**.
A confirmation warning appears.

Step 7 Click **Yes**.
DCNM removes the secure MAC address from the interface configuration. If you removed the last secure MAC address from a VLAN, that VLAN no longer appears in the Dynamic Address Configuration section.

You do not need to save your changes.

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 the maximum number of MAC addresses per VLAN on a Layer 2 interface. The largest maximum number of addresses that you can configure is 1025 addresses.

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.

Before You Begin

Port security must be enabled globally.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 If the interface that you want to configure does not appear, do the following:

a) From the menu bar, choose **Actions ➤ Add Interface**.
Below the selected interface type, a new row contains a drop-down list in the Interface column.

b) In the Interface column, from the drop-down list, choose the interface on which you want to enable port security.

The interface name appears in the new row of the Summary pane.

Step 4 Click the interface on which you want to configure the maximum number of secure MAC addresses.

Step 5 From the Details pane, click the **Secure Interface Details** tab.

Step 6 (Optional) If you want to configure the maximum number of secure MAC addresses for the interface, do the following:

a) Expand the **Secure Interface Configuration** section, if necessary.
b) In the Maximum Number of Address field, enter the new maximum number.

Step 7 (Optional) If you want to configure the maximum number of secure MAC addresses for a VLAN on the interface, do the following:

a) Expand the **Secure Address Configuration** section, if necessary.
b) If the VLAN that you need does not appear, right-click either on an existing VLAN entry or on a blank row, choose **Add VLAN**, and then from the drop-down list, choose the VLAN ID.
c) In the Maximum Number of Secure Addresses column, double-click the entry for the VLAN and enter the new maximum number.

Step 8 (Optional) From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.
DCNM configures the interface with the secure MAC address maximums that you specified.

Related Topics

- Removing a Dynamic or Sticky Secure MAC Address, page 15
- Removing a Static Secure MAC Address on an Interface, page 14

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

Port security must be enabled globally.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 If the interface that you want to configure does not appear, do the following:

a) From the menu bar, choose **Actions ➤ Add Interface**.
Below the selected interface type, a new row contains a drop-down list in the Interface column.

b) In the Interface column, from the drop-down list, choose the interface on which you want to enable port security.

The interface name appears in the new row of the Summary pane.

Step 4 Click the interface on which you want to configure secure MAC address aging.

Step 5 From the Details pane, click the **Dynamic MAC Addresses** tab.

Step 6 From the Aging Type drop-down list, pick the aging type.

Step 7 In the Age field, enter the number of minutes for the aging period.

Step 8 From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.
DCNM configures the interface with the secure MAC address aging type and time that you specified.

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

Port security must be enabled globally.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 If the interface that you want to configure does not appear, do the following:

a) From the menu bar, choose **Actions ➤ Add Interface**.
Below the selected interface type, a new row contains a drop-down list in the Interface column.

b) In the Interface column, from the drop-down list, choose the interface on which you want to enable port security.

The interface name appears in the new row of the Summary pane.

Step 4 Click the interface on which you want to configure the security violation action.

Step 5 From the Details pane, click the **Secure Interface Details** tab and then expand the **Secure Interface Configuration** section, if necessary.

Step 6 In the Interface Setting area, from the Violation Action drop-down list, choose the security violation action.

Step 7 (Optional) From the menu bar, choose **File ➤ Deploy** to apply your changes to the device.

Displaying Secure MAC Addresses

You can display secure MAC addresses for an interface.

Procedure

Step 1 From the Feature Selector pane, choose **Switching ➤ Layer 2 Security ➤ Port Security**.
The available devices appear in the Summary pane.

Step 2 Do one of the following:

- If you want to configure a physical interface, expand ***Device*** **➤ Physical Interfaces ➤** ***Slot***.
- If you want to configure a port-channel interface, expand ***Device*** **➤ Port Channels**.

Interfaces with port security enabled appear, in addition to other interfaces that were previously added to the port security summary table.

Step 3 Click the interface.
The Secure Interface Details tab and the Dynamic MAC Addresses tab appear in the Details pane.

Step 4 (Optional) To display dynamic or sticky secure MAC addresses, click the **Dynamic MAC Addresses** tab.
The Dynamic MAC Addresses tab displays the Host MAC Address table. If the interface is in trunk port mode, DCNM groups the dynamic or sticky secure MAC addresses by VLAN.

Step 5 (Optional) To display static secure MAC addresses, click the **Secure Interface Details** tab and then expand the **Secure Address Configuration** section, if necessary.
The Secure MAC Addresses tab displays the Host MAC Address table. If the interface is in trunk port mode, DCNM groups the static secure MAC addresses by VLAN.

Field Descriptions for Port Security

Device: Global Settings Tab

Table 1: Device: Global Settings Tab

Field	Description
Enable Port Security service	Link that enables the port security feature globally on the device. This link appears only when port security is not enabled on the selected device. By default, port security is not enabled.
Stop learning	Whether dynamic secure MAC address learning is globally permitted on the device. By default, this check box is unchecked.

Interface: Secure Interface Details: Secure Interface Configuration Section

Table 2: Interface: Secure Interface Details: Secure Interface Configuration Section

Field	Description
Interface	*Display only.* Name of the physical interface. Appears only when the interface is a physical interface.
Port Channel	*Display only.* Name of the port-channel interface. Appears only when the interface is a port-channel interface.
Access VLAN	*Display only.* Access VLAN for the interface. Appears only when the interface is in access mode.
Port Security Configured VLANs	*Display only.* VLANs that packets using the interface can belong to. Appears only when the interface is in trunk mode.
Host Primary VLAN	*Display only.* Primary VLAN for the interface. Appears only when the interface is a physical interface in PVLAN host mode.

Field	Description
Promiscuous Primary VLAN	*Display only.* Primary VLAN for the interface. Appears only when the interface is a physical interface in PVLAN promiscuous mode.
Port Type	*Display only.* Port mode of the interface. Possible values are as follows: • Access • Trunk • PVLAN Host (physical interfaces only) • PVLAN Promiscuous (physical interfaces only) **Note** Port security does not support interfaces in Routed port mode.
Violation Action	Action that the device takes when it detects a security violation on the interface. You can choose one of the following settings: • Protect • Restrict • Shutdown (Default)
Secure Address Count	
Maximum number of addresses	Number of secure MAC addresses allowed on the interface. The default is one secure MAC address.
Number of configured MAC addresses	*Display only.* Number of static secure MAC addresses configured for the interface.
Number of learnt MAC addresses	*Display only.* Number of dynamic or sticky secure MAC addresses learned for the interface.

Interface: Secure Interface Details: Secure Address Configuration Section

Table 3: Interface: Secure Interface Details: Secure Address Configuration Section

Field	Description
VLAN ID	*Display only.Trunk mode only.* ID of the VLAN on which the MAC address is secured.
Maximum Number of Secure Addresses	*Trunk mode only.* Maximum number of secure MAC addresses allowed on the VLAN for the interface.
Number of configured MAC addresses	*Trunk mode only.* Number of static secure MAC addresses on the VLAN for the interface.
Number of learnt MAC addresses	*Trunk mode only.* Number of sticky or dynamic secure MAC addresses on the VLAN for the interface.
Host MAC Address	Static secure MAC address. Valid entries are dotted hexadecimal MAC addresses. By default, there are no static secure MAC addresses.

Interface: Dynamic MAC Addresses Tab

Table 4: Interface: Dynamic MAC Addresses Tab

Field	Description
Interface	*Display only.* Physical interface name. Appears only when the interface is a physical interface.
Port Channel	*Display only.* Port-channel interface name. Appears only when the interface is a port-channel interface.
Port Type	*Display only.* Port mode of the interface. Possible values are as follows: • Access • Trunk • PVLAN Host (physical interfaces only)

Field	Description
	• PVLAN Promiscuous (physical interfaces only) **Note** Port security does not support interfaces in Routed port mode.
Aging Type	Aging type for dynamically learned, secure MAC addresses. You can choose one of the following settings: • Absolute—Addresses age based how long ago the device learned the address. This is the default setting. • InActivity—Addresses age based on how long ago the device last received traffic from the MAC address on the current interface.
Age	Aging time, in minutes, for dynamically learned, secure MAC addresses. Valid entries are whole numbers from 1 to 1440.
Dynamic MAC Stickiness	Whether the device learns secure MAC address by the sticky method. If this field is selected, the devices stores addresses that it learns in NVRAM. By default, the device learns addresses by the dynamic method.
Host MAC Address	*Display only.* MAC addresses secured by the dynamic or sticky address learning method.

Additional References for Port Security

Related Documents

Related Topic	Document Title
Layer 2 switching	*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 4.2*Cisco DCNM Layer 2 Switching Configuration Guide, Release 4.2

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
• CISCO-PORT-SECURITY-MIB **Note** Traps are supported for notification of secure MAC address violations.	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for Port Security

This table lists the release history for this feature.

Table 5: Feature History for Port Security

Feature Name	Releases	Feature Information
Port security	4.2(1)	Support for Layer 2 port-channel interfaces was added.