# Configuring 802.1X

This chapter contains the following sections:

# Information About 802.1X

802.1X defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a Cisco NX-OS device port.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

## Device Roles

With 802.1X port-based authentication, the devices in the network have specific roles.

**Figure 1: 802.1X Device Roles**

This figure shows the device roles in 802.1X.
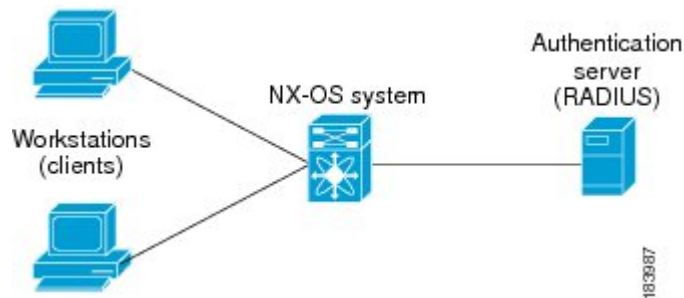
The specific roles are as follows:

**Supplicant**

The client device that requests access to the LAN and Cisco NX-OS device services and responds to requests from the Cisco NX-OS device. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating device.

**Note** To resolve Windows XP network connectivity and Cisco 802.1X port-based authentication issues, read the Microsoft Knowledge Base article at this URL: http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

**Authentication server**

The authentication server performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the Cisco NX-OS device regarding whether the supplicant is authorized to access the LAN and Cisco NX-OS device services. Because the Cisco NX-OS device acts as the proxy, the authentication service is transparent to the supplicant. The Remote Authentication Dial-In User Service (RADIUS) security device with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server, version 3.0. RADIUS uses a supplicant-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

**Authenticator**

The authenticator controls the physical access to the network based on the authentication status of the supplicant. The authenticator acts as an intermediary (proxy) between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the requested identity information with the authentication server, and relaying a response to the supplicant. The authenticator includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the authenticator receives EAPOL frames and relays them to the authentication server, the authenticator strips off the Ethernet header and encapsulates the remaining EAP frame in the RADIUS format. This encapsulation process does not modify or examine the EAP frames, and the authentication server must support EAP within the native frame format. When the authenticator receives frames from the authentication server, the authenticator removes the server's frame header, leaving the EAP frame, which the authenticator then encapsulates for Ethernet and sends to the supplicant.

**Note** The Cisco NX-OS device can only be an 802.1X authenticator.

# Authentication Initiation and Message Exchange

Either the authenticator (Cisco NX-OS device) or the supplicant (client) can initiate authentication. If you enable authentication on a port, the authenticator must initiate authentication when it determines that the port link state transitions from down to up. The authenticator then sends an EAP-request/identity frame to the supplicant to request its identity (typically, the authenticator sends an initial identity/request frame followed by one or more requests for authentication information). When the supplicant receives the frame, it responds with an EAP-response/identity frame.

If the supplicant does not receive an EAP-request/identity frame from the authenticator during bootup, the supplicant can initiate authentication by sending an EAPOL-start frame, which prompts the authenticator to request the supplicant's identity.

**Note**   If 802.1X is not enabled or supported on the network access device, the Cisco NX-OS device drops any EAPOL frames from the supplicant. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant transmits data as if the port is in the authorized state. A port in the authorized state means that the supplicant has been successfully authenticated.

When the supplicant supplies its identity, the authenticator begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the authenticator port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used.

*Figure 2: Message Exchange*

This figure shows a message exchange initiated by the supplicant using the One-Time-Password (OTP) authentication method with a RADIUS server. The OTP authentication device uses a secret pass-phrase to generate a sequence of one-time (single use)



passwords.

The user's secret pass-phrase never crosses the network at any time such as during authentication or during pass-phrase changes.

# Authenticator PAE Status for Interfaces

When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.

# Ports in Authorized and Unauthorized States

The authenticator port state determines if the supplicant is granted access to the network. The port starts in the unauthorized state. In this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a supplicant is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the supplicant to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the authenticator requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

Ports can have the following authorization states:

**Force authorized**
> Disables 802.1X port-based authentication and transitions to the authorized state without requiring any authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This authorization state is the default.

**Force unauthorized**
> Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The authenticator cannot provide authentication services to the client through the interface.

**Auto**
> Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received from the supplicant. The authenticator requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each supplicant that attempts to access the network is uniquely identified by the authenticator by using the supplicant's MAC address.

If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the authenticator can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and the supplicant is not granted network access.

When a supplicant logs off, it sends an EAPOL-logoff message, which causes the authenticator port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

# MAC Authentication Bypass

You can configure the Cisco NX-OS device to authorize a supplicant based on the supplicant MAC address by using the MAC authentication bypass feature. For example, you can enable this feature on interfaces configured for 802.1X that are connected to devices such as printers.

If 802.1X authentication times out while waiting for an EAPOL response from the supplicant, the Cisco NX-OS device tries to authorize the client by using MAC authentication bypass.

When you enable the MAC authentication bypass feature on an interface, the Cisco NX-OS device uses the MAC address as the supplicant identity. The authentication server has a database of supplicant MAC addresses that are allowed network access. After detecting a client on the interface, the Cisco NX-OS device waits for an Ethernet packet from the client. The Cisco NX-OS device sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the Cisco NX-OS device grants the client access to the network.

If an EAPOL packet is detected on the interface during the lifetime of the link, the Cisco NX-OS device determines that the device connected to that interface is an 802.1X-capable supplicant and uses 802.1X authentication (not MAC authentication bypass) to authorize the interface. EAPOL history is cleared if the interface link status goes down.

If the Cisco NX-OS device already authorized an interface by using MAC authentication bypass and detects an 802.1X supplicant, the Cisco NX-OS device does not unauthorize the client connected to the interface. When reauthentication occurs, the Cisco NX-OS device uses 802.1X authentication as the preferred reauthentication process if the previous session ended because the Termination-Action RADIUS attribute value is DEFAULT.

Clients that were authorized with MAC authentication bypass can be reauthenticated. The reauthentication process is the same as that for clients that were authenticated with 802.1X. During reauthentication, the port remains in the previously assigned VLAN. If reauthentication is successful, the switch keeps the port in the same VLAN.

If reauthentication is based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]) and if the Termination-Action RADIUS attribute (Attribute [29]) action is Initialize (the attribute value is DEFAULT), the MAC authentication bypass session ends, and connectivity is lost during reauthentication. If MAC authentication bypass is enabled and the 802.1X authentication times out, the switch uses the MAC authentication bypass feature to initiate reauthorization. For more information about these AV pairs, see RFC 3580, *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*.

MAC authentication bypass interacts with the following features:

- 802.1X authentication—You can enable MAC authentication bypass only if 802.1X authentication is enabled on the port.

- Port security— You can configure 802.1X authentication and port security on the same Layer 2 ports.

- Network admission control (NAC) Layer 2 IP validation—This feature takes effect after an 802.1X port is authenticated with MAC authentication bypass, including hosts in the exception list.

# 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.

# Single Host and Multiple Hosts Support

The 802.1X feature can restrict traffic on a port to only one endpoint device (single-host mode) or allow traffic from multiple endpoint devices on a port (multi-host mode).

Single-host mode allows traffic from only one endpoint device on the 802.1X port. Once the endpoint device is authenticated, the Cisco NX-OS device puts the port in the authorized state. When the endpoint device leaves the port, the Cisco NX-OS device put the port back into the unauthorized state. A security violation in 802.1X is defined as a detection of frames sourced from any MAC address other than the single MAC address authorized as a result of successful authentication. In this case, the interface on which this security association violation is detected (EAPOL frame from the other MAC address) will be disabled. Single host mode is

applicable only for host-to-switch topology and when a single host is connected to the Layer 2 (Ethernet access port) or Layer 3 port (routed port) of the Cisco NX-OS device.

Only the first host has to be authenticated on the 802.1X port configured with multiple host mode. The port is moved to the authorized state after the successful authorization of the first host. Subsequent hosts are not required to be authorized to gain network access once the port is in the authorized state. If the port becomes unauthorized when reauthentication fails or an EAPOL logoff message is received, all attached hosts are denied access to the network. The capability of the interface to shut down upon security association violation is disabled in multiple host mode. This mode is applicable for both switch-to-switch and host-to-switch topologies.

## Supported Topologies

The 802.1X port-based authentication is supported in two topologies:

   • Point-to-point

   • Wireless LAN

In a point-to-point configuration, only one supplicant (client) can connect to the 802.1X-enabled authenticator (Cisco NX-OS device) port. The authenticator detects the supplicant when the port link state changes to the up state. If a supplicant leaves or is replaced with another supplicant, the authenticator changes the port link state to down, and the port returns to the unauthorized state.

**Figure 3: Wireless LAN Example**

This figure shows 802.1X port-based authentication in a wireless LAN. The 802.1X port is configured as a multiple-host port that becomes authorized as soon as one supplicant is authenticated.
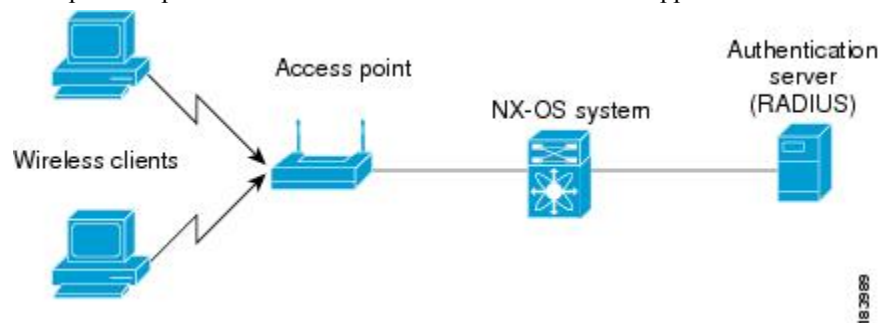


When the port is authorized, all other hosts indirectly attached to the port are granted access to the network. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the Cisco NX-OS device denies access to the network to all of the attached supplicants.

# Licensing Requirements for 802.1X

The following table shows the licensing requirements for this feature:

| Product | License Requirement |
|---------|---------------------|
| Cisco NX-OS | 802.1X requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*. |

# Prerequisites for 802.1X

802.1X has the following prerequisites:

• Cisco Nexus Release 6.0(2)N1(2) software.

• One or more RADIUS servers are accessible in the network.

• 802.1X supplicants are attached to the ports, unless you enable MAC address authentication bypass.

# 802.1X Guidelines and Limitations

802.1X port-based authentication has the following configuration guidelines and limitations:

• The Cisco NX-OS software supports 802.1X authentication only on physical ports.

• The Cisco NX-OS software does not support 802.1X authentication on port channels or subinterfaces.

• The Cisco NX-OS software supports 802.1X authentication on member ports of a port channel but not on the port channel itself.

• The Cisco NX-OS software does not support the following 802.1X configurations on port channel members when the members are configured for 802.1X:

  • Single-host mode cannot be configured on member ports of a port channel. Only multi-host mode is supported on member ports of a port channel.

  • MAC authentication bypass cannot be enabled on the member ports.

  • Port security cannot be configured on the port channel.

• Member ports with and without 802.1X configuration can coexist in a port channel. However, you must ensure the identical 802.1X configuration on all the member ports in order for channeling to operate with 802.1X.

• When you enable 802.1X authentication, supplicants are authenticated before any other Layer 2 or Layer 3 features are enabled on an Ethernet interface.

• The Cisco NX-OS software supports 802.1X authentication only on Ethernet interfaces that are in a port channel or a trunk or an access port.

• The Cisco NX-OS software does not support single host mode on trunk interfaces or member interfaces in a port channel.

• The Cisco NX-OS software does not support MAC address authentication bypass on trunk interfaces.

• The Cisco NX-OS software does not support MAC address authentication bypass on a port channel.

• The Cisco NX-OS software does not support Dot1X on vPC ports and MCT.

• The Cisco NX-OS software does not support the following 802.1X protocol enhancements:

  • One-to-many logical VLAN name to ID mapping

  • Web authorization

- Dynamic domain bridge assignment

- IP telephony

- Guest VLANs

# Default Settings for 802.1X

This table lists the default settings for 802.1X parameters.

**Table 1: Default 802.1X Parameters**

| Parameters | Default |
|---|---|
| 802.1X feature | Disabled |
| AAA 802.1X authentication method | Not configured |
| Per-interface 802.1X protocol enable state | Disabled (**force-authorized**)<br><br>**Note**     The port transmits and receives normal traffic without 802.1X-based authentication of the supplicant. |
| Periodic reauthentication | Disabled |
| Number of seconds between reauthentication attempts | 3600 seconds |
| Quiet timeout period | 60 seconds (number of seconds that the Cisco NX-OS device remains in the quiet state following a failed authentication exchange with the supplicant) |
| Retransmission timeout period | 30 seconds (number of seconds that the Cisco NX-OS device should wait for a response to an EAP request/identity frame from the supplicant before retransmitting the request) |
| Maximum retransmission number | 2 times (number of times that the Cisco NX-OS device will send an EAP-request/identity frame before restarting the authentication process) |
| Host mode | Single host |
| Supplicant timeout period | 30 seconds (when relaying a request from the authentication server to the supplicant, the amount of time that the Cisco NX-OS device waits for a response before retransmitting the request to the supplicant) |
| Authentication server timeout period | 30 seconds (when relaying a response from the supplicant to the authentication server, the amount of time that the Cisco NX-OS device waits for a reply before retransmitting the response to the server) |

# Configuring 802.1X

This section describes how to configure the 802.1X feature.

✎

**Note**    If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

## Process for Configuring 802.1X

This section describes the process for configuring 802.1X.

**Procedure**

**Step 1**    Enable the 802.1X feature.

**Step 2**    Configure the connection to the remote RADIUS server.

**Step 3**    Enable 802.1X feature on the Ethernet interfaces.

## Enabling the 802.1X Feature

You must enable the 802.1X feature on the Cisco NX-OS device before authenticating any supplicant devices.

**Procedure**

|  | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **feature dot1x**<br>**Example:**<br>`switch(config)# feature dot1x` | Enables the 802.1X feature. The default is disabled. |
| **Step 3** | **exit**<br>**Example:**<br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 4** | (Optional) **show dot1x**<br>**Example:**<br>`switch# show dot1x` | Displays the 802.1X feature status. |

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

# Configuring AAA Authentication Methods for 802.1X

You can use remote RADIUS servers for 802.1X authentication. You must configure RADIUS servers and RADIUS server groups and specify the default AAA authentication method before the Cisco NX-OS device can perform 802.1X authentication.

### Before you begin

Obtain the names or addresses for the remote RADIUS server groups.

### Procedure

| | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br><br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **aaa authentication dot1x default group** *group-list*<br><br>**Example:**<br><br>`switch(config)# aaa authentication dot1x`<br>`default group rad2` | Specifies the RADIUS server groups to use for 802.1X authentication.<br><br>The *group-list* argument consists of a space-delimited list of group names. The group names are the following:<br><br>   • **radius**—Uses the global pool of RADIUS servers for authentication.<br><br>   • *named-group* —Uses the global pool of RADIUS servers for authentication. |
| **Step 3** | **exit**<br><br>**Example:**<br><br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 4** | (Optional) **show radius-server**<br><br>**Example:**<br><br>`switch# show radius-server` | Displays the RADIUS server configuration. |

| | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 5** | (Optional) **show radius-server group** [*group-name*]<br><br>**Example:**<br>`switch# show radius-server group rad2` | Displays the RADIUS server group configuration. |
| **Step 6** | (Optional) **copy running-config startup-config**<br><br>**Example:**<br>`switch# copy running-config startup-config` | Copies the running configuration to the startup configuration. |

# Controlling 802.1X Authentication on an Interface

You can control the 802.1X authentication performed on an interface. An interface can have the following 802.1X authentication states:

**Auto**
> Enables 802.1X authentication on the interface.

**Force-authorized**
> Disables 802.1X authentication on the interface and allows all traffic on the interface without authentication. This state is the default.

**Force-unauthorized**
> Disallows all traffic on the interface.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

| | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot* / *port*<br><br>**Example:**<br>`switch(config)# interface ethernet 2/1`<br>`switch(config-if)#` | Selects the interface to configure and enters interface configuration mode. |
| **Step 3** | **dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**}<br><br>**Example:**<br>`switch(config-if)# dot1x port-control`<br>`auto` | Changes the 802.1X authentication state on the interface. The default is force-authorized. |

|  | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 4** | **exit**<br><br>**Example:**<br><br>```switch(config)# exit<br>switch#``` | Exits configuration mode. |
| **Step 5** | (Optional) **show dot1x all**<br><br>**Example:**<br><br>```switch# show dot1x all``` | Displays all 802.1X feature status and configuration information. |
| **Step 6** | (Optional) **show dot1x interface ethernet** *slot / port*<br><br>**Example:**<br><br>```switch# show dot1x interface ethernet<br>2/1``` | Displays 802.1X feature status and configuration information for an interface. |
| **Step 7** | (Optional) **copy running-config startup-config**<br><br>**Example:**<br><br>```switch# copy running-config<br>startup-config``` | Copies the running configuration to the startup configuration. |

# Configuring 802.1X Authentication on Member Ports

You can configure 802.1X authentication on the members of a port channel.

**Note**    You cannot configure 802.1X authentication on the port channel itself.

There are two ways to configure 802.1X authentication on member ports: 1) by configuring 802.1X on a member port and then adding the port to a port channel or 2) by creating a port channel, adding a port to the port channel, and then configuring 802.1X on the port. The following procedure provides instructions for the first method. To configure 802.1X using the second method, use these commands:

- **interface port-channel** *channel-number*

- **interface ethernet** *slot*/*port*

- **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]

- **dot1x port-control auto**

**Note**    For more information on the above commands, see the *Cisco NX-OS Interfaces Command Reference* for your platform.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

|  | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot*/*port*<br><br>**Example:**<br>`switch(config)# interface ethernet 7/1`<br>`switch(config-if)#` | Selects the interface to configure and enters interface configuration mode. |
| **Step 3** | **dot1x port-control auto**<br><br>**Example:**<br>`switch(config-if)# dot1x port-control`<br>`auto` | Changes the 802.1X authentication state on the interface. |
| **Step 4** | [**no**] **switchport**<br><br>**Example:**<br>`switch(config-if)# switchport` | Configures the interface as a Layer 2 port or, if you use the **no** keyword, as a Layer 3 port. |
| **Step 5** | **dot1x host-mode multi-host**<br><br>**Example:**<br>`switch(config-if)# dot1x host-mode`<br>`multi-host` | Enables multiple hosts mode for the interface. This command is required in order to add a port to a port channel. |
| **Step 6** | **channel-group** *channel-number* [**force**] [**mode** {**on** \| **active** \| **passive**}]<br><br>**Example:**<br>`switch(config-if)# channel-group 5 force` | Configures the port in a channel group and sets the mode. The channel number range is from 1 to 4096.The Cisco NX-OS software creates the port channel associated with this channel group if the port channel does not already exist.<br><br>The optional **force** keyword allows you to force an interface with some incompatible configurations to join the channel. The forced interface must have the same speed, duplex, and flow control settings as the channel group.<br><br>**Note** To remove an 802.1X-enabled port from a port channel, use the **no channel-group** *channel-number* command. |
| **Step 7** | **exit**<br><br>**Example:** | Exits interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | ```switch(config-if)# exit```<br>```switch(config)#``` | |
| Step 8 | **exit**<br>**Example:**<br>```switch(config)# exit```<br>```switch#``` | Exits global configuration mode. |
| Step 9 | (Optional) **show dot1x all**<br>**Example:**<br>```switch# show dot1x all``` | Displays all 802.1X feature status and configuration information. |
| Step 10 | (Optional) **show dot1x interface ethernet** *slot*/*port*<br>**Example:**<br>```switch# show dot1x interface ethernet 7/1``` | Displays 802.1X feature status and configuration information for an interface. |
| Step 11 | (Optional) **copy running-config startup-config**<br>**Example:**<br>```switch# copy running-config startup-config``` | Copies the running configuration to the startup configuration. |

# Creating or Removing an Authenticator PAE on an Interface

You can create or remove the 802.1X authenticator port access entity (PAE) instance on an interface.

**Note** By default, the Cisco NX-OS software creates the authenticator PAE instance on the interface when you enable 802.1X on an interface.

**Before you begin**

Enable the 802.1X feature.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **configure terminal**<br>**Example:**<br>```switch# configure terminal```<br>```switch(config)#``` | Enters global configuration mode. |

| | **Command or Action** | **Purpose** |
|---|---|---|
| Step 2 | (Optional) **show dot1x interface ethernet** *slot*/*port*<br><br>**Example:**<br><br>`switch# show do1x interface ethernet 2/1` | Displays the 802.1X configuration on the interface. |
| Step 3 | **interface ethernet** *slot*/*port*<br><br>**Example:**<br><br>`switch(config)# interface ethernet 2/1`<br>`switch(config-if)#` | Selects the interface to configure and enters interface configuration mode. |
| Step 4 | [**no**] **dot1x pae authenticator**<br><br>**Example:**<br><br>`switch(config-if)# dot1x pae`<br>`authenticator` | Creates an authenticator PAE instance on the interface. Use the **no** form to remove the PAE instance from the interface.<br><br>**Note** If an authenticator PAE already exists on the interface the **dot1x pae authentication** command does not change the configuration on the interface. |
| Step 5 | (Optional) **copy running-config startup-config**<br><br>**Example:**<br><br>`switch(config)# copy running-config`<br>`startup-config` | Copies the running configuration to the startup configuration. |

# Enabling Periodic Reauthentication for an Interface

You can enable periodic 802.1X reauthentication on an interface and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication defaults to the global value.

**Note** During the reauthentication process, the status of an already authenticated supplicant is not disrupted.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

| | **Command or Action** | **Purpose** |
|---|---|---|
| Step 1 | **configure terminal**<br><br>**Example:**<br><br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **interface ethernet** *slot/port*<br><br>**Example:**<br>`switch(config)# interface ethernet 2/1`<br>`switch(config-if)#` | Selects the interface to configure and enters interface configuration mode. |
| **Step 3** | **dot1x re-authentication**<br><br>**Example:**<br>`switch(config-if)# dot1x`<br>`re-authentication` | Enables periodic reauthentication of the supplicants connected to the interface. By default, periodic authentication is disabled. |
| **Step 4** | (Optional) **dot1x timeout re-authperiod** *seconds*<br><br>**Example:**<br>`switch(config-if)# dot1x timeout`<br>`re-authperiod 3300` | Sets the number of seconds between reauthentication attempts. The default is 3600 seconds. The range is from 1 to 65535.<br><br>**Note**      This command affects the behavior of the Cisco NX-OS device only if you enable periodic reauthentication on the interface. |
| **Step 5** | **exit**<br><br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits configuration mode. |
| **Step 6** | (Optional) **show dot1x all**<br><br>**Example:**<br>`switch(config)# show dot1x all` | Displays all 802.1X feature status and configuration information. |
| **Step 7** | (Optional) **copy running-config startup-config**<br><br>**Example:**<br>`switch(config)# copy running-config`<br>`startup-config` | Copies the running configuration to the startup configuration. |

# Manually Reauthenticating Supplicants

You can manually reauthenticate the supplicants for the entire Cisco NX-OS device or for an interface.

**Note** During the reauthentication process, the status of an already authenticated supplicant is not disrupted.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

|        | Command or Action | Purpose |
|--------|-------------------|---------|
| Step 1 | **dot1x re-authenticate** [**interface** *slot*/*port*]<br><br>**Example:**<br><br>`switch# dot1x re-authenticate interface 2/1` | Reauthenticates the supplicants on the Cisco NX-OS device or on an interface. |

# Manually Initializing 802.1X Authentication

You can manually initialize the authentication for all supplicants on a Cisco NX-OS device or for a specific interface.

**Note**  Initializing the authentication clears any existing authentication status before starting the authentication process for the client.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

|        | Command or Action | Purpose |
|--------|-------------------|---------|
| Step 1 | **dot1x initialize** [**interface ethernet** *slot*/*port*]<br><br>**Example:**<br><br>`switch# dot1x initialize interface ethernet 2/1` | Initializes 802.1X authentication on the Cisco NX-OS device or on a specified interface. |

# Changing 802.1X Authentication Timers for an Interface

You can change the following 802.1X authentication timers on the Cisco NX-OS device interfaces:

**Quiet-period timer**
>   When the Cisco NX-OS device cannot authenticate the supplicant, the switch remains idle for a set period of time and then tries again. The quiet-period timer value determines the idle period. An authentication failure might occur because the supplicant provided an invalid password. You can provide a faster response time to the user by entering a smaller number than the default. The default is the value of the global quiet period timer. The range is from 1 to 65535 seconds.

**Rate-limit timer**
>   The rate-limit period throttles EAPOL-Start packets from supplicants that are sending too many EAPOL-Start packets. The authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated for the rate-limit period duration. The default value is 0 seconds and the authenticator processes all EAPOL-Start packets. The range is from 1 to 65535 seconds.

**Switch-to-authentication-server retransmission timer for Layer 4 packets**

The authentication server notifies the switch each time that it receives a Layer 4 packet. If the switch does not receive a notification after sending a packet, the Cisco NX-OS device waits a set period of time and then retransmits the packet. The default is 30 seconds. The range is from 1 to 65535 seconds.

**Switch-to-supplicant retransmission timer for EAP response frames**

The supplicant responds to the EAP-request/identity frame from the Cisco NX-OS device with an EAP-response/identity frame. If the Cisco NX-OS device does not receive this response, it waits a set period of time (known as the retransmission time) and then retransmits the frame. The default is 30 seconds. The range is from 1 to 65535 seconds.

**Switch-to-supplicant retransmission timer for EAP request frames**

The supplicant notifies the Cisco NX-OS device it that received the EAP request frame. If the authenticator does not receive this notification, it waits a set period of time and then retransmits the frame. The default is the value of the global retransmission period timer. The range is from 1 to 65535 seconds.

---

**Note**   You should change the default values only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.

---

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

|  | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br><br>```switch# configure terminal```<br>```switch(config)#``` | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot*/*port*<br><br>**Example:**<br><br>```switch(config)# interface ethernet 2/1```<br>```switch(config-if)``` | Selects the interface to configure and enters interface configuration mode. |
| **Step 3** | (Optional) **dot1x timeout quiet-period** *seconds*<br><br>**Example:**<br><br>```switch(config-if)# dot1x timeout```<br>```quiet-period 25``` | Sets the number of seconds that the authenticator waits for a response to an EAP-request/identity frame from the supplicant before retransmitting the request. The default is the global number of seconds set for all interfaces. The range is from 1 to 65535 seconds. |
| **Step 4** | (Optional) **dot1x timeout ratelimit-period** *seconds*<br><br>**Example:**<br><br>```switch(config-if)# dot1x timeout```<br>```ratelimit-period 10``` | Sets the number of seconds that the authenticator ignores EAPOL-Start packets from supplicants that have successfully authenticated. The default value is 0 seconds. The range is from 1 to 65535 seconds. |

| | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 5** | (Optional) **dot1x timeout server-timeout** *seconds*<br><br>**Example:**<br>`switch(config-if)# dot1x timeout server-timeout 60` | Sets the number of seconds that the Cisco NX-OS device waits before retransmitting a packet to the authentication server. The default is 30 seconds. The range is from 1 to 65535 seconds. |
| **Step 6** | (Optional) **dot1x timeout supp-timeout** *seconds*<br><br>**Example:**<br>`switch(config-if)# dot1x timeout supp-timeout 20` | Sets the number of seconds that the Cisco NX-OS device waits for the supplicant to respond to an EAP request frame before the Cisco NX-OS device retransmits the frame. The default is 30 seconds. The range is from 1 to 65535 seconds. |
| **Step 7** | (Optional) **dot1x timeout tx-period** *seconds*<br><br>**Example:**<br>`switch(config-if)# dot1x timeout tx-period 40` | Sets the number of seconds between the retransmission of EAP request frames when the supplicant does not send notification that it received the request. The default is the global number of seconds set for all interfaces. The range is from 1 to 65535 seconds. |
| **Step 8** | **exit**<br><br>**Example:**<br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 9** | (Optional) **show dot1x all**<br><br>**Example:**<br>`switch# show dot1x all` | Displays the 802.1X configuration. |
| **Step 10** | (Optional) **copy running-config startup-config**<br><br>**Example:**<br>`switch# copy running-config startup-config` | Copies the running configuration to the startup configuration. |

# Enabling Single Host or Multiple Hosts Mode

You can enable single host or multiple hosts mode on an interface.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

|  | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot/port*<br>**Example:**<br>`switch(config)# interface ethernet 2/1`<br>`switch(config-if)` | Selects the interface to configure and enters interface configuration mode. |
| **Step 3** | **dot1x host-mode** {**multi-host** \| **single-host**}<br>**Example:**<br>`switch(config-if)# dot1x host-mode`<br>`multi-host` | Configures the host mode. The default is single-host.<br><br>**Note**      Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface. |
| **Step 4** | **exit**<br>**Example:**<br>`switch(config-if)# exit`<br>`switch(config)#` | Exits configuration mode. |
| **Step 5** | (Optional) **show dot1x all**<br>**Example:**<br>`switch# show dot1x all` | Displays all 802.1X feature status and configuration information. |
| **Step 6** | (Optional) **copy running-config startup-config**<br>**Example:**<br>`switch(config)# copy running-config`<br>`startup-config` | Copies the running configuration to the startup configuration. |

# Enabling MAC Authentication Bypass

You can enable MAC authentication bypass on an interface that has no supplicant connected.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

|  | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | switch# configure terminal<br>switch(config)# | |
| **Step 2** | **interface ethernet** *slot*/*port*<br><br>**Example:**<br><br>switch(config)# interface ethernet 2/1<br>switch(config-if) | Selects the interface to configure and enters interface configuration mode. |
| **Step 3** | **dot1x mac-auth-bypass** [**eap**]<br><br>**Example:**<br><br>switch(config-if)# dot1x mac-auth-bypass | Enables MAC authentication bypass. The default is bypass disabled. Use the **eap** keyword to configure the Cisco NX-OS device to use EAP for authorization. |
| **Step 4** | **exit**<br><br>**Example:**<br><br>switch(config-if)# exit<br>switch(config)# | Exits configuration mode. |
| **Step 5** | (Optional) **show dot1x all**<br><br>**Example:**<br><br>switch# show dot1x all | Displays all 802.1X feature status and configuration information. |
| **Step 6** | (Optional) **copy running-config startup-config**<br><br>**Example:**<br><br>switch(config)# copy running-config<br>startup-config | Copies the running configuration to the startup configuration. |

# Disabling 802.1X Authentication on the Cisco NX-OS Device

You can disable 802.1X authentication on the Cisco NX-OS device. By default, the Cisco NX-OS software enables 802.1X authentication after you enable the 802.1X feature. However, when you disable the 802.1X feature, the configuration is removed from the Cisco NX-OS device. The Cisco NX-OS software allows you to disable 802.1X authentication without losing the 802.1X configuration.

**Note** When you disable 802.1X authentication, the port mode for all interfaces defaults to force-authorized regardless of the configured port mode. When you reenable 802.1X authentication, the Cisco NX-OS software restores the configured port mode on the interfaces.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

|        | **Command or Action**                                 | **Purpose**                                                                 |
|--------|-------------------------------------------------------|-----------------------------------------------------------------------------|
| Step 1 | **configure terminal**                                | Enters global configuration mode.                                           |
|        | **Example:**                                          |                                                                             |
|        | `switch# configure terminal`<br>`switch(config)#`     |                                                                             |
| Step 2 | **no dot1x system-auth-control**                      | Disables 802.1X authentication on the Cisco NX-OS device. The default is enabled. |
|        | **Example:**                                          |                                                                             |
|        | `switch(config)# no dot1x`<br>`system-auth-control`   | **Note**    Use the **dot1x system-auth-control** command to enable 802.1X authentication on the Cisco NX-OS device. |
| Step 3 | **exit**                                              | Exits configuration mode.                                                   |
|        | **Example:**                                          |                                                                             |
|        | `switch(config)# exit`<br>`switch#`                   |                                                                             |
| Step 4 | (Optional) **show dot1x**                             | Displays the 802.1X feature status.                                         |
|        | **Example:**                                          |                                                                             |
|        | `switch# show dot1x`                                  |                                                                             |
| Step 5 | (Optional) **copy running-config startup-config**     | Copies the running configuration to the startup configuration.             |
|        | **Example:**                                          |                                                                             |
|        | `switch# copy running-config`<br>`startup-config`     |                                                                             |

# Disabling the 802.1X Feature

You can disable the 802.1X feature on the Cisco NX-OS device.

When you disable 802.1X, all related configurations are automatically discarded. The Cisco NX-OS software creates an automatic checkpoint that you can use if you reenable 802.1X and want to recover the configuration. For more information, see the *Cisco NX-OS System Management Configuration Guide* for your platform.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

|        | **Command or Action**   | **Purpose**                       |
|--------|-------------------------|-----------------------------------|
| Step 1 | **configure terminal**  | Enters global configuration mode. |
|        | **Example:**            |                                   |

|         | **Command or Action**                                      | **Purpose**                                              |
|---------|-----------------------------------------------------------|----------------------------------------------------------|
|         | `switch# configure terminal`<br>`switch(config)#`         |                                                          |
| **Step 2** | **no feature dot1x**<br><br>**Example:**<br><br>`switch(config)# no feature dot1x` | Disables 802.1X.<br><br>**Caution**   Disabling the 802.1X feature removes all 802.1X configuration. |
| **Step 3** | **exit**<br><br>**Example:**<br><br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 4** | (Optional) **copy running-config startup-config**<br><br>**Example:**<br><br>`switch# copy running-config`<br>`startup-config` | Copies the running configuration to the startup configuration. |

# Setting the Maximum Authenticator-to-Supplicant Frame Retransmission Retry Count for an Interface

You can set the maximum number of times that the Cisco NX-OS device retransmits authentication requests to the supplicant on an interface before the session times out. The default is 2 times and the range is from 1 to 10.

### Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

### Procedure

|         | **Command or Action**                                      | **Purpose**                                              |
|---------|-----------------------------------------------------------|----------------------------------------------------------|
| **Step 1** | **configure terminal**<br><br>**Example:**<br><br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot*/*port*<br><br>**Example:**<br><br>`switch(config)# interface ethernet 2/1`<br>`switch(config-if)#` | Selects the interface to configure and enters interface configuration mode. |
| **Step 3** | **dot1x max-req** *count*<br><br>**Example:**<br><br>`switch(config-if)# dot1x max-req 3` | Changes the maximum authorization request retry count. The default is 2 times and the range is from 1 to 10. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note**      Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface. |
| **Step 4** | **exit**<br><br>**Example:**<br><br>`switch(config)# exit`<br>`switch#` | Exits interface configuration mode. |
| **Step 5** | (Optional) **show dot1x all**<br><br>**Example:**<br><br>`switch# show dot1x all` | Displays all 802.1X feature status and configuration information. |
| **Step 6** | (Optional) **copy running-config startup-config**<br><br>**Example:**<br><br>`switch(config)# copy running-config`<br>`startup-config` | Copies the running configuration to the startup configuration. |

# Enabling RADIUS Accounting for 802.1X Authentication

You can enable RADIUS accounting for the 802.1X authentication activity.

### Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br><br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **dot1x radius-accounting**<br><br>**Example:**<br><br>`switch(config)# dot1x radius-accounting` | Enables RADIUS accounting for 802.1X. The default is disabled. |
| **Step 3** | **exit**<br><br>**Example:**<br><br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | (Optional) **show dot1x**<br><br>**Example:**<br>`switch# show dot1x` | Displays the 802.1X configuration. |
| **Step 5** | (Optional) **copy running-config startup-config**<br><br>**Example:**<br>`switch# copy running-config`<br>`startup-config` | Copies the running configuration to the startup configuration. |

# Configuring AAA Accounting Methods for 802.1X

You can enable AAA accounting methods for the 802.1X feature.

### Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal** | Enters global configuration mode. |
| **Step 2** | **aaa accounting dot1x default group** *group-list* | Configures AAA accounting for 802.1X. The default is disabled.<br><br>The *group-list* argument consists of a space-delimited list of group names. The group names are the following:<br><br>• **radius**—For all configured RADIUS servers.<br><br>• *named-group*—Any configured RADIUS server group name. |
| **Step 3** | **exit** | Exits configuration mode. |
| **Step 4** | (Optional) **show aaa accounting** | Displays the AAA accounting configuration. |
| **Step 5** | (Optional) **copy running-config startup-config** | Copies the running configuration to the startup configuration. |

### Example

This example shows how to enable the 802.1x feature:

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group radius
switch(config)# exit
```

```
switch# show aaa accounting
switch# copy running-config startup-config
```

# Setting the Maximum Reauthentication Retry Count on an Interface

You can set the maximum number of times that the Cisco NX-OS device retransmits reauthentication requests to the supplicant on an interface before the session times out. The default is 2 times and the range is from 1 to 10.

### Before you begin

Enable the 802.1X feature on the Cisco NX-OS device.

### Procedure

|        | Command or Action | Purpose |
|--------|-------------------|---------|
| **Step 1** | **configure terminal** <br><br> **Example:** <br> `switch# configure terminal` <br> `switch(config)#` | Enters global configuration mode. |
| **Step 2** | **interface ethernet** *slot*/*port* <br><br> **Example:** <br> `switch(config)# interface ethernet 2/1` <br> `switch(config-if)#` | Selects the interface to configure and enters interface configuration mode. |
| **Step 3** | **dot1x max-reauth-req** *retry-count* <br><br> **Example:** <br> `switch(config-if)# dot1x max-reauth-req` <br> ` 3` | Changes the maximum reauthentication request retry count. The default is 2 times and the range is from 1 to 10. |
| **Step 4** | **exit** <br><br> **Example:** <br> `switch(config)# exit` <br> `switch#` | Exits interface configuration mode. |
| **Step 5** | (Optional) **show dot1x all** <br><br> **Example:** <br> `switch# show dot1x all` | Displays all 802.1X feature status and configuration information. |
| **Step 6** | (Optional) **copy running-config startup-config** <br><br> **Example:** <br> `switch(config)# copy running-config` <br> `startup-config` | Copies the running configuration to the startup configuration. |

# Verifying the 802.1X Configuration

To display 802.1X information, perform one of the following tasks:

| Command | Purpose |
|---|---|
| **show dot1x** | Displays the 802.1X feature status. |
| **show dot1x all** [**details** | **statistics** | **summary**] | Displays all 802.1X feature status and configuration information. |
| **show dot1x interface ethernet** *slot/port* [**details** | **statistics** | **summary**] | Displays the 802.1X feature status and configuration information for an Ethernet interface. |
| **show running-config dot1x** [**all**] | Displays the 802.1X feature configuration in the running configuration. |
| **show startup-config dot1x** | Displays the 802.1X feature configuration in the startup configuration. |

For detailed information about the fields in the output from these commands, see the *Cisco NX-OS Security Command Reference* for your platform.

# Monitoring 802.1X

You can display the statistics that the Cisco NX-OS device maintains for the 802.1X activity.

**Before you begin**

Enable the 802.1X feature on the Cisco NX-OS device.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **show dot1x** {**all** | **interface ethernet** *slot/port*} **statistics**<br><br>**Example:**<br>`switch# show dot1x all statistics` | Displays the 802.1X statistics. |

# Configuration Example for 802.1X

The following example shows how to configure 802.1X for an access port:

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
```

```
dot1x port-control auto
```

The following example shows how to configure 802.1X for a trunk port:

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
dot1x port-control auto
dot1x host-mode multi-host
```

**Note**  Repeat the **dot1x pae authenticator**  and **dot1x port-control auto** commands for all interfaces that require 802.1X authentication.

# Additional References for 802.1X

This section includes additional information related to implementing 802.1X.

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco NX-OS Licensing | *Cisco NX-OS Licensing Guide* |
| Command reference | *Cisco Nexus 5000 Series NX-OS Security Command Reference* |
| VRF configuration | *Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration guide* |

### Standards

| Standards | Title |
|---|---|
| IEEE Std 802.1X- 2004 (Revision of IEEE Std 802.1X-2001) | *802.1X IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control* |
| RFC 2284 | *PPP Extensible Authentication Protocol (EAP)* |
| RFC 3580 | *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* |

### MIBs

| MIBs | MIBs Link |
|---|---|
| • IEEE8021-PAE-MIB | To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml |

# Feature History for 802.1X

*Table 2: Feature History for 802.1X*

| Feature Name | Release | Feature Information |
|---|---|---|
| 802.1X | 6.0(2)N1(2) | This feature was introduced. |