



Configuring 802.1x Authentication

This chapter describes how to configure 802.1x authentication on the Catalyst 4000 family switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 4500 Series, Catalyst 2948G, and Catalyst 2980G Switches Command Reference* publication.



Note

For information on configuring ports to allow or restrict traffic based on host MAC addresses, see Chapter 16, “[Configuring Port Security](#).”



Note

For information on configuring authentication, authorization, and accounting (AAA) to monitor and control access to the command-line interface (CLI) on the Catalyst 4000 family switches, see Chapter 30, “[Configuring the Switch Access Using AAA](#).”

This chapter consists of these sections:

- [Understanding How 802.1x Authentication Works](#), page 31-1
- [Authentication Default Configuration](#), page 31-7
- [Authentication Configuration Guidelines](#), page 31-8
- [Configuring 802.1x Authentication on the Switch](#), page 31-8

Understanding How 802.1x Authentication Works

IEEE 802.1x is a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a local area network (LAN) through publicly accessible ports. 802.1x authenticates each user device that is connected to a switch port before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. Only EAPOL traffic is allowed to pass through the uncontrolled port, which is

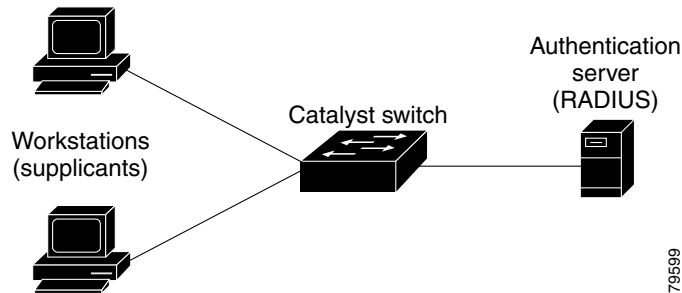
always open. The controlled port is open *only* when the device that is connected to the port has been authorized by 802.1x. After this authorization takes place, the controlled port opens, allowing normal traffic to pass. You can restrict traffic in both directions or just incoming traffic.

The following sections describe how 802.1x authentication work.

Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles. (See [Figure 31-1](#).)

Figure 31-1 802.1x Device Roles



- *Host*—Requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1x-compliant software.



Note IEEE 802.1x uses the term *supplicant* for *client* or *host*. In this publication, we use *host* instead of *supplicant* because *host* is used in the Catalyst 4000 family CLI syntax.

- *Authentication server*—Performs the actual authentication of the host. The authentication server validates the identity of the host and notifies the switch whether or not the host is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the host. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system 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 operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- *Switch*—Controls the physical access to the network based on the authentication status of the host. The switch acts as an intermediary (proxy) between the host and the authentication server, requesting identity information from the host, verifying that information with the authentication server, and relaying a response to the host. The switch interacts with the RADIUS client. The RADIUS client encapsulates and decapsulates the EAP frames and interacts with the authentication server.

When the switch receives Extensible Authentication Protocol over LAN (EAPOL) frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is reencapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the host.

Authentication Initiation and Message Exchange

The switch or the host can initiate authentication. If you enable authentication on a port by using the `set port dot1x mod/port port-control auto` command, the switch must initiate authentication when it determines that the port link state transitions from down to up. The switch sends an EAP-request/identity frame to the host to request its identity (typically, the switch sends an initial identity/request frame that is followed by one or more requests for authentication information). When the host receives the frame, it sends an EAP-response/identity frame.

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



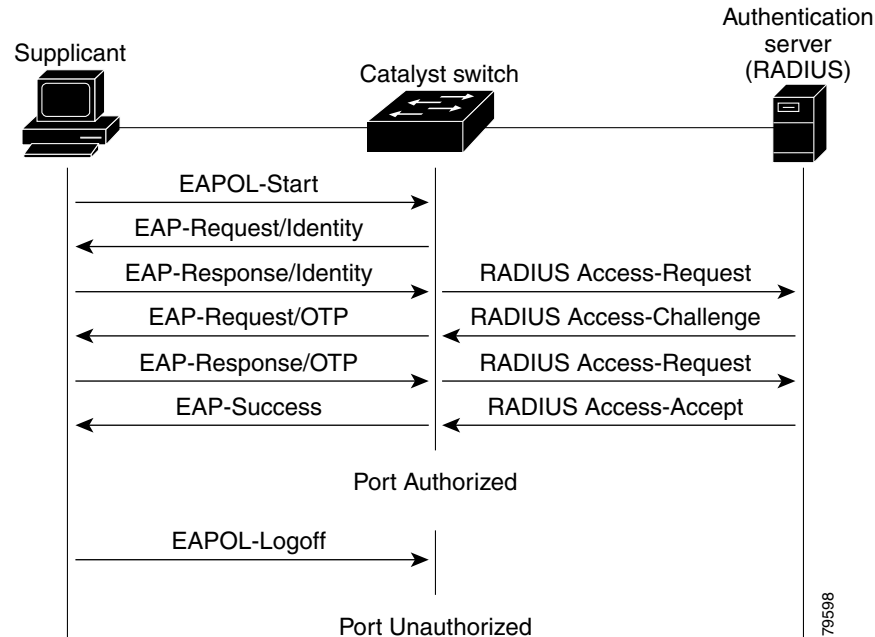
Note

If 802.1x is not enabled or supported on the network access device, any EAPOL frames from the host are dropped. If the host does not receive an EAP-request/identity frame after three attempts to start authentication, the host transmits frames as if the port is in the authorized state. A port that is in the authorized state means that the host has been successfully authenticated. For more information, see the [“Ports in Authorized and Unauthorized States”](#) section on page 31-4.

When the host supplies its identity, the switch acts as the intermediary, passing EAP frames between the host and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. For more information, see the [“Ports in Authorized and Unauthorized States”](#) section on page 31-4.

The specific exchange of EAP frames depends on the authentication method that is being used. [Figure 31-2](#) shows a message exchange that is initiated by the host using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 31-2 Message Exchange



Ports in Authorized and Unauthorized States

The switch port state determines if the host 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 host is successfully authenticated, the port transitions to the *authorized* state, allowing all traffic for the host to flow normally.

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

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

You control the port authorization state by using the **set port dot1x mod/port port-control** command and these keywords:

- **force-authorized**—Disables 802.1x authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the host. This is the default setting.
- **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the host to authenticate. The switch cannot provide authentication services to the host through the interface.
- **auto**—Enables 802.1x 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. The switch requests the identity of the host and begins relaying authentication messages between the host and the authentication server. Each host attempting to access the network is uniquely identified by the switch by using the host's MAC address.

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

When a host logs off, the server sends an EAPOL-logoff message, causing the switch 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.

[Table 31-1](#) defines the terms used in 802.1x.

Table 31-1 802.1x Terminology

Term	Definition
Authenticator PAE	(Referred to as the “authenticator”) entity at one end of a point-to-point LAN segment that enforces host authentication. The authenticator is independent of the actual authentication method and functions only as a pass-through for the authentication exchange. It communicates with the host, submits the information from the host to the authentication server, and authorizes the host when instructed to do so by the authentication server.
Authentication server	Entity that provides the authentication service for the authenticator PAE. It checks the credentials of the host PAE, and then notifies its client, the authenticator PAE, whether the host PAE is authorized to access the LAN/switch services.
Authorized state	Status of the port after the host PAE is authorized.
Both	Bidirectional flow control, incoming and outgoing, at an unauthorized switch port.
Controlled port	Secured access point.
EAP	Extensible Authentication Protocol.
EAPOL ¹	Encapsulated EAP messages that can be handled directly by a LAN MAC service.
In	Flow control only on incoming frames in an unauthorized switch port.
Port	Single point of attachment to the LAN infrastructure (for example, MAC bridge ports).
PAE ²	Protocol object that is associated with a specific system port.
PDU	Protocol data unit.
RADIUS	Remote Access Dial In User Service.
PAE	(Referred to as the “host”) entity that requests access to the LAN/switch services and responds to information requests from the authenticator.
Unauthorized state	Status of the port before the host PAE is authorized.
Uncontrolled port	Unsecured access point that allows the uncontrolled exchange of PDUs.

1. EAPOL = Extensible Authorization Protocol over LAN

2. PAE = Port access entity

Authentication Server

The frames exchanged between the authenticator and the authentication server are dependent on the authentication mechanism, so they are not defined by the 802.1x standard. You can use other protocols, but we recommend RADIUS for authentication, particularly when the authentication server is located remotely, because RADIUS has extensions that support encapsulation of EAP frames built into it.

802.1x Parameters Configurable on the Switch

With 802.1x, you can do the following:

- Specify force-authorized port control, force-unauthorized port control, or automatic 802.1x port control
- Enable or disable multiple hosts on a specific port
- Enable or disable system authentication control
- Specify the quiet time interval
- Specify the authenticator to host retransmission time interval
- Specify the back-end authenticator to host retransmission time interval
- Specify the back-end authenticator to authentication server retransmission time interval
- Specify the number of frames that are retransmitted from the back-end authenticator to host
- Specify the automatic host reauthentication time interval
- Specify the port shutdown timeout period after a security violation
- Enable or disable automatic host reauthentication

802.1x VLAN Assignment Using a RADIUS Server

In software release 6.3 or earlier releases, once the 802.1x host is authenticated, it joins an NVRAM-configured VLAN. With software release 7.2(1) and later releases, after authentication, an 802.1x host can receive its VLAN assignment from the RADIUS server.

The VLAN assignment feature allows you to restrict users to a specific VLAN. For example, you could put guest users in a VLAN with limited access to the network.

802.1x authenticated ports are assigned to a VLAN based on the username of the host that is connected to the port. The VLAN assignment feature works with the RADIUS server, which has a database of username-to-VLAN mappings.

After a successful 802.1x authentication of the port, the RADIUS server sends the VLAN in which the user needs to be given access. 802.1x port behavior with the VLAN assignment feature is summarized as follows:

- At linkup, the server places an 802.1x port in its original NVRAM-configured VLAN.
- After linkup, the server can put the port in the RADIUS-supplied VLAN if the RADIUS-supplied VLAN is valid and active in the management domain.
- If the port is currently in a different VLAN, the port is moved to the RADIUS-supplied VLAN.
- If the RADIUS-supplied VLAN is not active in the management domain, the server puts the port in an inactive state.
- If the RADIUS-supplied VLAN is invalid or there is a problem with the port hardware, the server moves the port to the 802.1x unauthorized state.
- If you enabled the multiple hosts option on an 802.1x port, the server places all hosts in the same RADIUS-supplied VLAN received by the first authenticated user.
- When an 802.1x-configured module goes down, the server clears all Enhanced Address Recognition Logic (EARL) entries for 802.1x ports.

- When an 802.1x-configured module comes up, the server configures all 802.1x ports in NVRAM-configured VLANs.
- If you clear an 802.1x-configured module's configuration, all the 802.1x ports are moved to the NVRAM-configured VLAN and all the EARL entries for the 802.1x ports are cleared.
- If you move an 802.1x port from an authorized to an unauthorized state, the server moves the port to the NVRAM-configured VLAN.

In order for the 802.1x VLAN assignment using a RADIUS server to successfully complete, the RADIUS server must return the following three RFC 2868 attributes back to the authenticator (the Cisco switch to which the host attaches):

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-Id = VLAN NAME

Attribute [64] must contain the value "VLAN" (type 13). Attribute [65] must contain the value "802" (type 6). Attribute [81] specifies the VLAN name in which the successfully authenticated 802.1x host should be put.

**Note**

You must specify the VLAN by its name and not by its number.

Authentication Default Configuration

Table 31-2 shows the default configuration for authentication.

Table 31-2 802.1x Authentication Default Configuration

Feature	Default Value
802.1x port control	Force-Authorized
802.1x multiple hosts	Disabled
802.1x system authentication control	Enable
802.1x quiet period time	60 sec
802.1x authenticator to host retransmission time	30 sec
802.1x back-end authenticator to host retransmission time	30 sec
802.1x back-end authenticator to authentication server retransmission time	30 sec
802.1x number of frames retransmitted from back-end authenticator to host	2 frames
802.1x automatic host reauthentication time	3600 sec
802.1x automatic authenticator reauthentication of host	Disabled
802.1x shutdown timeout period	0 seconds

Authentication Configuration Guidelines

This section provides the guidelines for configuring 802.1x authentication on the switch:

- 802.1x will work with other protocols, but we recommend that you use RADIUS with a remotely located authentication server.
- 802.1x is supported only on Ethernet ports.
- You cannot enable 802.1x on a trunk port until you turn off the trunking feature on that port. You cannot enable trunking on an 802.1x port.
- You cannot enable 802.1x on a dynamic port until you turn off the DVLAN feature on that port. You cannot enable DVLAN on an 802.1x port.
- You cannot enable 802.1x on a channeling port until you turn off the channeling feature on that port. You cannot enable channeling on an 802.1x port.
- You cannot enable 802.1x on a switched port analyzer (SPAN) destination port, and you cannot configure SPAN destination on an 802.1x port. However, you can configure an 802.1x port as a SPAN source port.

Configuring 802.1x Authentication on the Switch

The following sections describe how to configure 802.1x authentication on the switch.

Enabling 802.1x Globally

You must enable 802.1x authentication for the entire system before configuring it for individual ports. After you globally enable 802.1x authentication, you can configure individual ports for 802.1x authentication if they meet the specific requirements that are required by 802.1x. To enable 802.1x authentication for individual ports, see the [“Enabling and Initializing 802.1x Authentication for Individual Ports” section on page 31-9](#).

To globally enable 802.1x authentication, perform this task in privileged mode:

Task	Command
Globally enable 802.1x.	set dot1x system-auth-control enable

This example shows how to globally enable 802.1x authentication:

```
Console> (enable) set dot1x system-auth-control enable
dot1x system-auth-control enabled.
```

Disabling 802.1x Globally

When 802.1x authentication is enabled for the entire system, you can disable it globally. When 802.1x authentication is disabled globally, it is no longer available at any port, even ports that were previously configured for it.

To globally disable 802.1x authentication, perform this task in privileged mode:

Task	Command
Globally disable 802.1x.	set dot1x system-auth-control disable

This example shows how to globally disable 802.1x authentication:

```
Console> (enable) set dot1x system-auth-control disable
dot1x system-auth-control disabled.
```

Enabling and Initializing 802.1x Authentication for Individual Ports

After 802.1x authentication is globally enabled, you can enable and initialize 802.1x authentication from the console only for individual ports. To globally enable 802.1x authentication, see the “[Enabling 802.1x Globally](#)” section on page 31-8.



Note

You must specify at least one RADIUS server before you can enable 802.1x authentication on the switch. For information on specifying a RADIUS server, see the “[Specifying RADIUS Servers](#)” section on page 30-23.

To enable and initialize 802.1x authentication for access to the switch, perform this task in privileged mode:

	Task	Command
Step 1	Enable 802.1x control on a specific port.	set port dot1x mod/port port-control auto
Step 2	Initialize 802.1x on the same port.	set port dot1x mod/port initialize
Step 3	Verify the 802.1x configuration.	show port dot1x mod/port

This example shows how to enable 802.1x authentication on port 1 in module 4, initialize 802.1x authentication on the same port, and verify the configuration:

```
Console> (enable) set port dot1x 4/1 port-control auto
Port 4/1 dot1x port-control is set to auto.
Trunking disabled for port 4/1 due to Dot1x feature.
Spanntree port fast start option enabled for port 4/1.
Console> (enable) set port dot1x 4/1 initialize
Port 4/1 initializing...
Port 4/1 dot1x initialization complete.
Console> show port dot1x 4/1
Port  Auth-State      BEnd-State  Port-Control  Port-Status
-----
  4/1  connecting        finished    auto          unauthorized

Port  Multiple-Host  Re-authentication
-----
  4/1  disabled        disabled
```

Setting and Enabling Automatic Reauthentication of the Host

You can specify how often 802.1x authentication reauthenticates the host if you do so prior to enabling automatic 802.1x host reauthentication. If you do not specify a time period prior to enabling host reauthentication, 802.1x defaults to 3600 seconds (the valid values are from 1–65,535 seconds).

You can enable automatic 802.1x host reauthentication for hosts that are connected to a specific port. To manually reauthenticate the host that is connected to a specific port, see the [“Manually Reauthenticating the Host” section on page 31-10](#).

To set how often 802.1x authentication reauthenticates the host and enable automatic 802.1x reauthentication, perform this task in privileged mode:

	Task	Command
Step 1	Set the time constant for reauthenticating the host.	set dot1x re-authperiod <i>seconds</i>
Step 2	Enable reauthentication.	set port dot1x mod/port re-authentication enable
Step 3	Verify the 802.1x configuration.	show port dot1x mod/port

This example shows how to set automatic reauthentication to 7200 seconds, enable 802.1x reauthentication, and verify the configuration:

```

Console> (enable) set dot1x re-authperiod 7200
dot1x re-authperiod set to 7200 seconds
Console> (enable) set port dot1x 4/1 re-authentication enable
Port 4/1 re-authentication enabled.
Console> (enable) show port dot1x 4/1
Port  Auth-State      BEnd-State Port-Control      Port-Status
-----
 4/1  connecting        finished   auto                unauthorized
Port  Multiple Host Re-authentication
-----
 4/1  disabled          enabled

```

Manually Reauthenticating the Host

You can manually reauthenticate the host that is connected to a specific port at any time. When you want to configure automatic 802.1x host reauthentication, see the [“Setting and Enabling Automatic Reauthentication of the Host” section on page 31-10](#).

To manually reauthenticate a host that is connected to a specific port, perform this task in privileged mode:

Task	Command
Manually reauthenticate the host that is connected to a specific port.	set port dot1x mod/port re-authenticate

This example shows how to manually reauthenticate the host that is connected to port 1 on module 4:

```

Console> (enable) set port dot1x 4/1 re-authenticate
Port 4/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 4/1 authorized.

```

Enabling Multiple Hosts

You can enable a specific port to allow multiple-user access. When a port is enabled for multiple users, and a host that is connected to that port is authorized successfully, any host (with any MAC address) is allowed to send and receive traffic on that port. If you then connect multiple hosts to that port through a hub, you can reduce the security level on that port.

To enable multiple-user access on a specific port, perform this task in privileged mode:

Task	Command
Enable multiple hosts on a specific port.	set port dot1x <i>mod/port</i> multiple-host enable

This example shows how to enable access for multiple hosts on port 1 on module 4:

```
Console> (enable) set port dot1x 4/1 multiple-host enable
Port 4/1 multiple hosts allowed.
```

Disabling Multiple Hosts

You can disable multiple-user access on any port where it is enabled.

To disable multiple-user access on a specific port, perform this task in privileged mode:

Task	Command
Disable multiple hosts on a specific port.	set port dot1x <i>mod/port</i> multiple-host disable

This example shows how to disable access for multiple hosts on port 1 on module 4:

```
Console> (enable) set port dot1x 4/1 multiple-host disable
Port 4/1 multiple hosts not allowed.
```

Setting the Quiet Period

When the authenticator cannot authenticate the host, it remains idle for a set period of time and then tries again. The idle time is determined by the quiet-period value. (The default is 60 seconds.) You may set the value from 0–65,535 seconds.

To set the value for the quiet period, perform this task in privileged mode:

Task	Command
Set the quiet-period value.	set dot1x quiet-period <i>seconds</i>

This example shows how to set the quiet period to 45 seconds:

```
Console> (enable) set dot1x quiet-period 45
dot1x quiet-period set to 45 seconds.
```

Setting the Authenticator-to-Host Retransmission Time for EAP-Request/Identity Frames

The host notifies the authenticator that it received the EAP-request/identity frame. When the authenticator does not receive this notification, the authenticator waits a set period of time and then retransmits the frame. You may set the amount of time that the authenticator waits for notification from 1 to 65,535 seconds. The default is 30 seconds.

To set the authenticator-to-host retransmission time for the EAP-request/identity frames, perform this task in privileged mode:

Task	Command
Set the authenticator-to-host retransmission time for EAP-request/identity frames.	set dot1x tx-period <i>seconds</i>

This example shows how to set the authenticator-to-host retransmission time for the EAP-request/identity frame to 15 seconds:

```
Console> (enable) set dot1x tx-period 15
dot1x tx-period set to 15 seconds.
```

Setting the Supplicant-to-Host Retransmission Time for EAP-Request Frames

The host notifies the back-end authenticator that it received the EAP-request frame. When the back-end authenticator does not receive this notification, the back-end authenticator waits a set period of time, and then retransmits the frame. You may set the amount of time that the back-end authenticator waits for notification from 1–65,535 seconds. The default is 30 seconds.

To set the back-end authenticator-to-host retransmission time for the EAP-request frames, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-host retransmission time for EAP-request frame.	set dot1x supp-timeout <i>seconds</i>

This example shows how to set the back-end authenticator-to-host retransmission time for the EAP-request frame to 15 seconds:

```
Console> (enable) set dot1x supp-timeout 15
dot1x supp-timeout set to 15 seconds.
```

Setting the Back-End Authenticator-to-Authentication-Server Retransmission Time for Transport Layer Packets

The authentication server notifies the back-end authenticator each time it receives a transport layer packet. When the back-end authenticator does *not* receive a notification after sending a packet, the back-end authenticator waits a set period of time, and then retransmits the packet. You may set the amount of time that the back-end authenticator waits for notification from 1–65,535 seconds. The default is 30 seconds.

To set the value for the retransmission of transport layer packets from the back-end authenticator to the authentication server, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-authentication-server retransmission time for transport layer packets.	set dot1x server-timeout <i>seconds</i>

This example shows how to set the value for the retransmission time for transport layer packets that are sent from the back-end authenticator to the authentication server to 15 seconds:

```
Console> (enable) set dot1x server-timeout 15
dot1x server-timeout set to 15 seconds.
```

Setting the Back-End Authenticator-to-Host Frame-Retransmission Number

The authentication server notifies the back-end authenticator each time that it receives a specific number of frames. When the back-end authenticator does not receive this notification after sending the frames, the back-end authenticator waits a set period of time and then retransmits the frames. You may set the number of frames that the back-end authenticator retransmits from 1–10 (the default is 2).

To set the number of frames that are retransmitted from the back-end authenticator to the host, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-host frame retransmission number.	set dot1x max-req <i>count</i>

This example shows how to set the number of retransmitted frames that are sent from the back-end authenticator to the host to 4:

```
Console> (enable) set dot1x max-req 4
dot1x max-req set to 4.
```

Setting the Shutdown Timeout Period

If a port is shut down because of a security violation, you must either manually reenabte it or configure the shutdown timeout period after which the port can be enabled again.

To set the period of time that a port will be disabled after a security violation, perform this task in privileged mode:

Task	Command
Set the shutdown timeout period.	set dot1x shutdown-timeout <i>1- 65535 seconds</i>

This example shows how to set the shutdown timeout period:

```
Console> (enable) set dot1x shutdown-timeout 300
dot1x shutdown-timeout set to 300 seconds.
Console> (enable)
```

Setting the Back-End Authenticator-to-Host Frame-Retransmission Number

The authentication server notifies the back-end authenticator each time that it receives a specific number of frames. When the back-end authenticator does not receive this notification after sending the frames, the back-end authenticator waits a set period of time and then retransmits the frames. You may set the number of frames that the back-end authenticator retransmits from 1–10 (the default is 2).

To set the number of frames that are retransmitted from the back-end authenticator to the host, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-host frame retransmission number.	set dot1x max-req count

This example shows how to set the number of retransmitted frames that are sent from the back-end authenticator to the host to 4:

```
console> (enable) set dot1x max-req 4
dot1x max-req count set to 4.
Console> (enable)
```

Setting the Back-End Authenticator-to-Host Frame-Retransmission Number

The authentication server notifies the back-end authenticator each time that it receives a specific number of frames. When the back-end authenticator does not receive this notification after sending the frames, the back-end authenticator waits a set period of time and then retransmits the frames. You may set the number of frames that the back-end authenticator retransmits from 1–10 (the default is 2).

To set the number of frames that are retransmitted from the back-end authenticator to the host, perform this task in privileged mode:

Task	Command
Set the back-end authenticator-to-host frame retransmission number.	set dot1x max-req count

This example shows how to set the number of retransmitted frames that are sent from the back-end authenticator to the host to 4:

```
Console> (enable) set dot1x max-req 4
dot1x max-req set to 4.
```

Resetting the 802.1x Configuration Parameters to the Default Values

You can reset the 802.1x configuration parameters to the default values with a single command, which also globally disables 802.1x.

To reset the 802.1x configuration parameters to the default values, perform this task in privileged mode:

	Task	Command
Step 1	Reset the 802.1x configuration parameters to the default values and globally disable 802.1x.	clear dot1x config
Step 2	Verify the 802.1x configuration.	show dot1x

This example shows how to reset the 802.1x configuration parameters to the default values:

```
Console> (enable) clear dot1x config
This command will disable dot1x on all ports and take dot1x parameter values back to
factory defaults.
Do you want to continue (y/n) [n]?y
Dot1x config cleared.
Console> (enable) 2002 Sep 06 11:34:27 %SECURITY-1-DOT1X_BACKEND_SERVER:No RADIUS
servers configured
```

Setting the Trace Severity

You can alter the trace severity for 802.1x authentication. The number setting affects the number of trace messages that are displayed. Low numbers result in fewer messages; high numbers result in more messages.

To set the trace severity for 802.1x, perform this task in privileged mode:

Task	Command
Set the trace severity for 802.1x authentication.	set trace dot1x trace-level

This example shows how to set the trace severity for 802.1x authentication to 5:

```
Console> (enable) set trace dot1x 5
DOT1X tracing set to 5
```

Warning!! Turning on trace may affect the operation of the system.
Use with caution.

Using the show Commands

You can use these **show** commands to access information about 802.1x authentication and its configuration:

- **show port dot1x help**
- **show port dot1x**
- **show port dot1x statistics**
- **show dot1x**

To display the usage options for the **show port dot1x** command, perform this task in normal mode:

Task	Command
Display the usage options for the show port dot1x command.	show port dot1x help

This example shows how to display the usage options for the **show port dot1x** command:

```
Console> (enable) show port dot1x help
Usage: show port dot1x [<mod[/port]>]
       show port dot1x statistics [<mod[/port]>]
```

To display the values for all the parameters that are associated with the authenticator PAE and back-end authenticator on a specific port on a specific module, perform this task in normal mode:

Task	Command
Display the values for all configurable and current state parameters that are associated with the authenticator PAE and back-end authenticator on a specific port on a specific module.	show port dot1x mod/port

This example shows how to display the values for all the parameters that are associated with the authenticator PAE and back-end authenticator on port 1 on module 4:

```
Console> (enable) show port dot1x 4/1
Port  Auth-State          BEnd-State Port-Control      Port-Status
-----
 4/1  connecting             finished   auto                 unauthorized
Port  Multiple Host Re-authentication
-----
 4/1  disabled               enabled
```

To display the statistics for the different types of EAP frames that are transmitted and received by the authenticator on a specific port on a specific module, perform this task in normal mode:

Task	Command
Display the statistics for the different types of EAP frames that are transmitted and received by the authenticator on a specific port on a specific module.	show port dot1x statistics mod/port

This example shows how to display the statistics for the different types of EAP frames that are transmitted and received by the authenticator on port 1 on module 4:

```

Console> (enable) show port dot1x statistics 4/1
Port   Tx_Req/Id Tx_Req Tx_Total Rx_Start Rx_Logoff Rx_Resp/Id Rx_Resp
-----
4/1    97       0     97       0       0       0       0
Port   Rx_Invalid Rx_Len_Err Rx_Total Last_Rx_Frm_Ver Last_Rx_Frm_Src_Mac
-----
4/1    0         0         0         0         00-00-00-00-00-00

```

To display the global 802.1x parameters, perform this task in normal mode:

Task	Command
Display the PAE capabilities, protocol version, system-auth-control, and other global dot1x parameters.	show dot1x

This example shows how to display the global 802.1x parameters:

```

Console> (enable) show dot1x
PAE Capability           Authenticator Only
Protocol Version         1
system-auth-control      enabled
re-authentication        disabled
max-req                  2
quiet-period             60 seconds
re-authperiod            3600 seconds
server-timeout           30 seconds
supp-timeout             30 seconds
tx-period                30 seconds

```

