



Configuring 802.1x Authentication

This chapter describes how to configure 802.1x authentication on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.



Note

For information on configuring ports to allow or restrict traffic based on host MAC addresses, see Chapter 35, “[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 6500 series switches, see Chapter 21, “[Configuring the Switch Access Using AAA](#).”

This chapter consists of these sections:

- [Understanding How 802.1x Authentication Works](#), page 36-1
- [Authentication Default Configuration](#), page 36-11
- [Authentication Configuration Guidelines](#), page 36-11
- [Configuring 802.1x Authentication on the Switch](#), page 36-12

Understanding How 802.1x Authentication Works

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 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. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN 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.

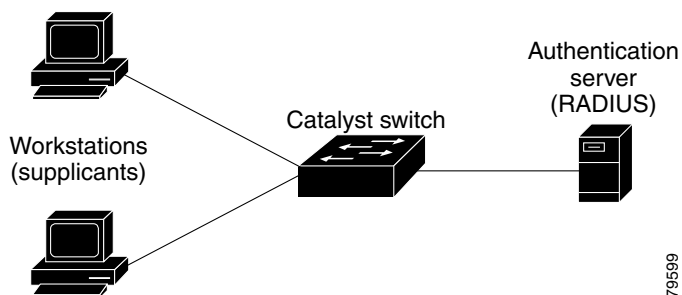
These sections provide the following information:

- [Device Roles](#), page 36-2
- [Authentication Initiation and Message Exchange](#), page 36-3
- [Ports in Authorized and Unauthorized States](#), page 36-4
- [Traffic Control](#), page 36-6
- [Authentication Server](#), page 36-6
- [802.1x Parameters Configurable on the Switch](#), page 36-6
- [802.1x VLAN Assignment Using a RADIUS Server](#), page 36-7
- [Using 802.1x Authentication with DHCP](#), page 36-8
- [Using 802.1x Authentication on Ports Configured for Auxiliary VLAN Traffic](#), page 36-8
- [Using 802.1x Authentication for Guest VLANs](#), page 36-8
- [Using 802.1x Authentication with Port Security](#), page 36-9
- [Using 802.1x Authentication with ARP Traffic Inspection](#), page 36-10

Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles. (See [Figure 36-1](#).)

Figure 36-1 802.1x Device Roles



- *Supplicant*—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 The IEEE 802.1x standard uses the term *supplicant* for *client* or *host*. In this publication, we use *host* instead of *supplicant* because *host* is used in the Catalyst 6500 series 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.



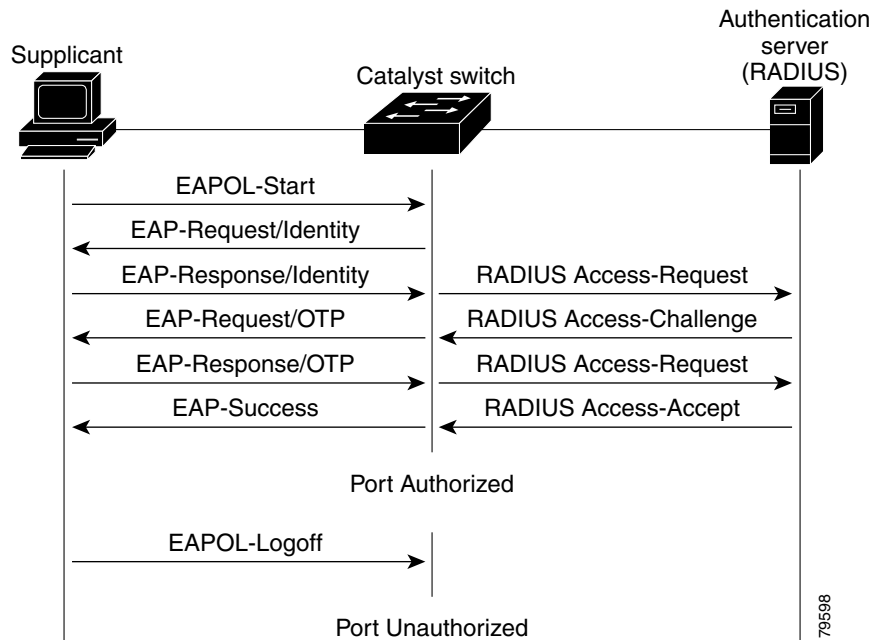
Note

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 36-4](#).

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 36-4](#).

The specific exchange of EAP frames depends on the authentication method being used. [Figure 36-2](#) shows a message exchange that is initiated by the host using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 36-2 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 36-1 defines the 802.1x terms.

Table 36-1 802.1x Terminology

Term	Definition
Authenticator PAE ¹	(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 ²	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	Protocol object that is associated with a specific system port.
PDU	Protocol data unit.
RADIUS	Remote Access Dial-In User Service.

Table 36-1 802.1x Terminology (continued)

Term	Definition
Supplicant ³ PAE	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 supplicant PAE is authorized.
Uncontrolled port	Unsecured access point that allows the uncontrolled exchange of PDUs.

1. PAE = port access entity
2. EAPOL = Extensible Authorization Protocol over LAN
3. The IEEE 802.1x standard uses the term *supplicant* for *client* or *host*. In this publication, we use *host* instead of *supplicant* because *host* is used in the Catalyst 6500 series CLI syntax.

Traffic Control

You can restrict traffic in both directions or just incoming traffic.

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

You can configure these 802.1x parameters on the switch:

- Specify Force-Authorized, Force-Unauthorized, or Automatic 802.1x port control
- Specify single authentication, multiple authentication, and multiple host authentication
- 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
- Enable or disable automatic host reauthentication

802.1x VLAN Assignment Using a RADIUS Server

In supervisor engine software releases prior to software release 7.2(2), once the 802.1x host is authenticated, it joins an NVRAM-configured VLAN. With software release 7.2(2) 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. This feature works with the RADIUS server that 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, an 802.1x port is placed in its original NVRAM-configured VLAN.
- After linkup, the port can be put 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, it is moved to the RADIUS-supplied VLAN.
- If the RADIUS-supplied VLAN is not active in the management domain, the port is put in an inactive state.
- If the RADIUS-supplied VLAN is invalid or there is a problem with the port hardware, the port is moved to the 802.1x unauthorized state.
- When the multiple hosts option is enabled on an 802.1x port, all hosts are placed in the same RADIUS-supplied VLAN that is received by the first authenticated user.
- When an 802.1x-configured module goes down, all Enhanced Address Recognition Logic (EARL) entries are cleared for 802.1x ports.
- When an 802.1x-configured module comes up, all 802.1x ports are configured in NVRAM-configured VLANs.
- When an 802.1x-configured module's configuration is cleared, all the 802.1x ports are moved to the NVRAM-configured VLAN and all the EARL entries for the 802.1x ports are cleared.
- When an 802.1x port moves from an authorized to an unauthorized state, the port is moved to the NVRAM-configured VLAN.

In order for the “802.1x VLAN Assignment Using a RADIUS Server” feature 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 or VLAN ID (VLAN number)



Note The VLAN ID attribute is in software release 7.6(8) and later releases.

Attribute [64] must contain the value “VLAN” (type 13). Attribute [65] must contain the value “802” (type 6). Attribute [81] specifies the VLAN name or VLAN ID in which the successfully authenticated 802.1x host is placed.

Using 802.1x Authentication with DHCP

802.1x authentication support for Dynamic Host Configuration Protocol (DHCP) makes it possible for the DHCP server to assign IP addresses to different classes of end users by adding the authenticated user identity into the DHCP discover process. This feature allows network administrators the ability to secure IP addresses given to end users for accounting purposes and to grant services based on Layer 3 criteria. Once the RADIUS server authenticates the supplicant, the DHCP server keeps an authenticated user identity that is associated with the IP address lease. This authenticated user identity is then added to the DHCP discover process so that different addresses can be assigned to different classes of users.

After successful 802.1x authentications between the supplicant and the RADIUS server, the switch puts the port in the forwarding state and stores the attributes it receives from the RADIUS server. These attributes are used to map to an address pool in the DHCP server. Because the switch can act as a DHCP Relay Agent, it can receive DHCP messages and regenerate those messages for transmission on another interface. When the supplicant does DHCP discovery (following authentication), the DHCP Relay Agent on the supervisor engine receives the packet and adds the stored attributes it received from the RADIUS server to the DHCP discovery packet and submits the discovery broadcast again. The mapping of user-to-IP address can be on a one-to-one, one-to-many, or many-to-many basis. The one-to-many mapping allows the same user to authenticate through 802.1x hosts on multiple ports.

Using 802.1x Authentication on Ports Configured for Auxiliary VLAN Traffic

You can enable 802.1x on a Multiple VLAN Access Port (MVAP), and you can enable an auxiliary VLAN ID on an 802.1x port.

Ports that are configured for 802.1x authentication and an auxiliary VLAN must be in single-host authentication mode to forward auxiliary VLAN-tagged packets from an IP phone. Because IP phones do not have host PAE capability, when auxiliary VLAN-tagged packets are received on a port that is configured for 802.1x authentication from the IP phone, the packets are forwarded as authorized traffic.

A host PAE that is connected behind an IP phone will be authenticated. Only traffic from the host PAE behind the IP phone will be forwarded after authentication.

**Note**

If a new host PAE is connected to an IP phone that is connected to an 802.1x-enabled auxiliary VLAN port, after removing the old host, the new host PAE will be authenticated. Only traffic from the new host PAE will be forwarded after authentication.

Using 802.1x Authentication for Guest VLANs

The guest VLAN feature enables non-802.1x capable hosts to access networks that use 802.1x authentication. For example, you can use the guest VLAN feature while you are upgrading your system to support 802.1x authentication.

When you configure a VLAN as an 802.1x guest VLAN, all non-802.1x capable hosts are put in this VLAN. You can configure any VLAN (except for private VLANs and RSPAN VLANs) as a guest VLAN. If a port is already forwarding on the guest VLAN and you enable 802.1x support on the network interface of the host, the port is immediately moved out of the guest VLAN and the authenticator waits for authentication to occur.

Enabling 802.1x authentication on a port starts the 802.1x protocol. If the host fails to respond to the packets from the authenticator within a certain amount of time, the authenticator puts the port in the guest VLAN.

Usage Guidelines for Using 802.1x Authentication with Guest VLANs on Windows-XP Hosts

The usage guidelines for using 802.1x authentication with guest VLANs on Windows-XP hosts are as follows:

- If the host fails to respond to the authenticator, the port will remain in the connecting state for 180 seconds. After this time period, the login/password window will not appear on the host. The workaround is to have the user unplug and then reconnect their network interface cable.
- Hosts that respond with an incorrect login/password will fail authentication. Hosts that fail authentication will not be put in the guest VLAN. The first time a host fails authentication, the quiet-period timer starts and no activity will occur for the duration of the quiet-period timer. When the quiet-period timer expires, the host is presented with the login/password window. If the host fails authentication for the second time, the quiet-period timer starts again and no activity will occur for the duration of the quiet-period timer. The host is presented with the login/password window a third time. If the host fails authentication the third time, the port is put in the connecting and unauthorized states. The workaround is to have the user unplug and then reconnect their network interface cable.

**Note**

Guest VLANs are limited to the local switch and are not propagated through VTP.

Using 802.1x Authentication with Port Security

802.1x authentication is compatible with the port security feature (for more information, see Chapter 35, “Configuring Port Security”). If you enable port security for only one MAC address on a specific port, only that MAC address will authenticate through a RADIUS server. Users connected through all other MAC addresses are denied access. If you enable port security for multiple MAC addresses, each address needs to authenticate through the 802.1x RADIUS server.

**Note**

Due to caveat CSCin25663, the MAC address that you configure for port security will be removed when a logoff message is received from that particular MAC address or that MAC address fails to reauthenticate. This problem will be resolved in a future software release.

**Note**

When 802.1x authentication and port security are enabled on any 802.1x port, the 802.1x authentication takes precedence over the port security on the port. That is, the host is authenticated first and then is secured by port security.

You can enable port security for any 802.1x mode (single-authentication, multiple-host, or multiple-authentication modes). Only one mode can be enabled on a port at a time. The default port mode is single-authentication mode.

You can disable port security for single-authentication and multiple-host modes. You cannot disable port security for multiple-authentication mode.

When 802.1x authentication is enabled on a port that is also enabled for MAC-address based port security, 802.1x authentication does not occur on the port unless the maximum allowable number of MAC addresses has been configured. If you configure less than the maximum allowable number of MAC addresses on a port that is also configured for 802.1x single-host mode authentication, the system generates a message asking if you want the configured MAC addresses to be removed. If you answer “yes” to this message, the MAC addresses that you configured for MAC address-based port security are removed and the port is authenticated using 802.1x authentication. If 802.1x authentication is enabled for any other mode, no message is created and the MAC addresses are retained.

With the multiple-authentication mode, all connected hosts are authenticated using 802.1x and secured using port security. 802.1x authenticates the MAC address and then gives the MAC address to port security to secure it. When a MAC address sends an EAPOL logoff packet, the MAC address is cleared from the port security tables.

Using 802.1x Authentication with ARP Traffic Inspection



Note

This feature is available only with Supervisor Engine 2 with PFC2 or Supervisor Engine 720 with PFC3.



Note

ARP traffic inspection and 802.1x configurations are mutually exclusive of one another.

You can use 802.1x authentication with ARP traffic inspection to provide an additional layer of port and user security by eliminating the possibility of malicious users/hosts corrupting the ARP tables of other hosts. After a successful 802.1x supplicant authentication, ARP traffic inspection, which binds the supplicant’s IP address and MAC address, is invoked and eliminates the spoofing possibility.

ARP is a simple protocol that does not have an authentication mechanism so there is no means to ensure that ARP requests and replies are genuine. Without an authentication mechanism, a malicious user/host can corrupt the ARP tables of the other hosts on the same VLAN in a Layer 2 network or bridge domain.

For example, user/Host A (the malicious user) can send unsolicited ARP replies (or gratuitous ARP packets) to other hosts on the subnet with the IP address of the default router and the MAC address of Host A. With some earlier operating systems, even if a host already has a static ARP entry for the default router, the newly advertised binding from Host A is learned. If Host A enables IP forwarding and forwards all packets from the “spoofed” hosts to the router and vice versa, then Host A can carry out a man-in-the-middle attack (for example, using the program `dsniff`) without the spoofed hosts realizing that all of their traffic is being sniffed.

In addition, ARP inspection can drop packets where the source Ethernet MAC address (in the Ethernet header) does not match the source MAC address in the ARP header. You can enable (or disable) this feature through the CLI by entering the **set security acl arp-inspection match-mac {enable [drop [log]] | disable}** command.

ARP traffic inspection allows you to configure a set of order-dependent rules within the security ACL (VACL) framework to prevent ARP table attacks. ARP traffic inspection compliments the 802.1x port authentication protocol, which first binds the MAC address of the authenticated client to the port, eliminating the possibility of spoofing additional MAC addresses by adding an IP to MAC address binding for additional spoof proofing.

To configure ARP traffic inspection, see the [“Inspecting ARP Traffic” section on page 16-29](#).

Authentication Default Configuration

Table 36-2 shows the default 802.1x authentication configuration.

Table 36-2 802.1x 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 seconds
802.1x authenticator to host retransmission time	30 seconds
802.1x back-end authenticator to host retransmission time	30 seconds
802.1x back-end authenticator to authentication server retransmission time	30 seconds
802.1x number of frames that are retransmitted from back-end authenticator to host	2
802.1x automatic host reauthentication time	3600 seconds
802.1x automatic authenticator reauthentication of host	Disabled

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.
- Software release 7.5(1) supports two in-band management interfaces, sc0 and sc1. 802.1x authentication always uses the sc0 interface as the identifier for the authenticator when communicating with the RADIUS server. 802.1x authentication is not supported with the sc1 interface.
- 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. You cannot configure SPAN destination on an 802.1x port. However, you can configure an 802.1x port as a SPAN source port.
- You cannot set the auxiliary VLAN to **dot1p** or **untagged**, and the auxiliary VLAN should not be equal to the native VLAN on the 802.1x-enabled port.
- You cannot enable the multiple-authentication option on an 802.1x-enabled auxiliary VLAN port. Enabling the multiple-host option on an 802.1x-enabled auxiliary VLAN is not recommended.

- Do not assign a guest VLAN equal to an auxiliary VLAN because an 802.1x-enabled auxiliary VLAN port will not be put into the guest VLAN if the auxiliary VLAN on the port is the same as the guest VLAN.

Configuring 802.1x Authentication on the Switch

These sections describe how to configure 802.1x authentication on the switch:



Note

For information on using a RADIUS server for VLAN assignment, see the [“802.1x VLAN Assignment Using a RADIUS Server”](#) section on page 36-7.

- [Enabling 802.1x Globally](#), page 36-12
- [Disabling 802.1x Globally](#), page 36-13
- [Enabling 802.1x Authentication for Individual Ports](#), page 36-13
- [Enabling Multiple 802.1x Authentications](#), page 36-14
- [Setting and Enabling Automatic Reauthentication of the Host](#), page 36-15
- [Manually Reauthenticating the Host](#), page 36-15
- [Enabling Multiple Hosts](#), page 36-16
- [Disabling Multiple Hosts](#), page 36-16
- [Setting the Quiet Period](#), page 36-17
- [Setting the Authenticator-to-Host Retransmission Time for EAP-Request/Identity Frames](#), page 36-17
- [Setting the Back-End Authenticator-to-Host Retransmission Time for EAP-Request Frames](#), page 36-17
- [Setting the Back-End Authenticator-to-Authentication-Server Retransmission Time for Transport Layer Packets](#), page 36-18
- [Setting the Back-End Authenticator-to-Host Frame-Retransmission Number](#), page 36-18
- [Resetting the 802.1x Configuration Parameters to the Default Values](#), page 36-19
- [Enabling 802.1x Authentication for the DHCP Relay Agent](#), page 36-19
- [Disabling 802.1x Authentication for DHCP Relay Agent](#), page 36-20
- [Configuring an 802.1x Guest VLAN](#), page 36-21
- [Using the show Commands](#), page 36-21

Enabling 802.1x Globally

You must enable 802.1x authentication for the entire system before you can configure 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 required by 802.1x. To enable 802.1x authentication for individual ports, see the [“Enabling 802.1x Authentication for Individual Ports”](#) section on page 36-13.

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

Task	Command
Globally enable 802.1x authentication.	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 authentication.	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 802.1x Authentication for Individual Ports

After 802.1x authentication is globally enabled, you must enable 802.1x authentication from the console for individual ports. To globally enable 802.1x authentication, see the [“Enabling 802.1x Globally”](#) section on page 36-12.



Note

You must specify at least one RADIUS server before you can enable 802.1x authentication on the switch. For information on how to specify a RADIUS server, see [Chapter 21, “Configuring the Switch Access Using AAA.”](#)

To enable 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 <i>mod/port</i> port-control auto
Step 2	Verify the 802.1x configuration.	show port dot1x <i>mod/port</i>

This example shows how to enable 802.1x authentication on port 1 in module 4 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.
Spantree port fast start option enabled for port 4/1.
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               disabled

```

**Note**

To clear the current state machines for a new authentication, use the **set port dot1x mod/port initialize** command.

Enabling Multiple 802.1x Authentications

You can specify multiple authentications so that more than one host can gain access to an 802.1x port. Multiple authentication is Cisco proprietary and allows multiple dot1x-hosts on a port; every host is authenticated separately. Use these guidelines when enabling multiple 802.1x authentications:

- Traffic from non-802.1x hosts on multiple authenticated ports is blocked.
- A guest VLAN cannot be enabled on multiple authenticated ports.
- Multiple authentication cannot be enabled on a MVAP.
- Multiple authenticated ports go into the port VLAN and will not go into a RADIUS-assigned VLAN.
- Port security needs to be enabled on a port before you can enable multiple authentications on the port.
- Port security cannot be disabled on a multiple authenticated port.
- Port security timers are used on multiple authenticated ports. Reauthentication timers are not used on multiple authenticated ports.

To enable multiple 802.1x authentications, perform this task in privileged mode:

	Task	Command
Step 1	Enable multiple 802.1x authentication on a specific port.	set port dot1x mod/port multiple-authentication {enable disable}
Step 2	Verify the 802.1x configuration.	show port dot1x mod/port

This example shows how to enable multiple 802.1x authentication on port 1 in module 3 and verify the configuration:

```

Console> (enable) set port dot1x 3/1 multiple-authentication enable
Enable PortSecurity before enabling multiple-authentication
Console> (enable) set port security 3/1 enable
Port 3/1 security enabled.
Trunking disabled for Port 3/1 due to Security Mode.
Console> (enable) set port dot1x 3/1 multiple-authentication enable
Dot1x multiple-authentication mode enabled
Console> (enable) show port dot1x 3/1

```

```

Port  Auth-State          BEnd-State  Port-Control  Port-Status
-----
 3/1  -                      -           force-authorized  -

Port  Port-Mode  Re-authentication
-----
 3/1  MultiAuth  disabled
Console> (enable)

```

Setting and Enabling Automatic Reauthentication of the Host

You can specify how often 802.1x authentication reauthenticates the host if you do so before you enable automatic 802.1x host reauthentication. If you do not specify a time period before you enable host reauthentication, 802.1x defaults to 3,600 seconds (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 36-15.

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 re-authentication enable
Step 3	Verify the 802.1x configuration.	show port dot1x <i>mod/port</i>

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 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 36-15.

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 <i>mod/port</i> 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 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 0–65535 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 1–65535 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 Back-End Authenticator-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 1–65535 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 the 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 that 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 1–65535 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.
```

Resetting the 802.1x Configuration Parameters to the Default Values

You can reset the 802.1x configuration parameters to the default values with the **clear dot1x config** command, which also removes 802.1x on all ports.

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 remove 802.1x on all ports.	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 and verify the configuration:

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

Enabling 802.1x Authentication for the DHCP Relay Agent

To enable the DHCP Relay Agent to send 802.1x parameters for a particular VLAN to the DHCP server, perform this task in privileged mode:

	Task	Command
Step 1	Enable 802.1x authentication for the DHCP Relay Agent. This command creates an ACE entry with the given ACL name. The ACL can have other ACE entries but DHCP ACE entries are given priority.	set security acl ip <i>acl_name</i> permit dot1x-dhcp
Step 2	Verify the 802.1x configuration.	show dot1x

This example shows how to create an ACL entry for 802.1x DHCP relay traffic:

```
Console> (enable) set security acl ip dhcp_relay permit dot1x-dhcp
Successfully configured Dot1x Dhcp ACL for dhcp_relay. Use 'commit' command to save
changes
```

This example shows that after you create the ACL entry, how to configure the ACL to allow other traffic than DHCP:

```
Console> (enable) set security acl ip dhcp_relay permit any
dhcp_relay editbuffer modified. Use 'commit' command to apply changes.
console> (enable)
```

This example shows how to commit the ACE to NVRAM:

```
Console> (enable) commit security acl dhcp_relay
Commit operation in progress
ACL 'dhcp_relay' successfully committed.
```

This example shows how to map the VLANs that should be applied to dhcp-relay-acl:

```
Console> (enable) set security acl map dhcp_relay 1-3,20
Mapping in progress...
ACL dhcp_relay successfully mapped to VLAN 1.
ACL dhcp_relay successfully mapped to VLAN 2.
ACL dhcp_relay successfully mapped to VLAN 3.
ACL dhcp_relay successfully mapped to VLAN 20.
```

The DHCP Relay Agent Information field will be added in the DHCP packet that is forwarded from the client to the server. VLANs that are not mapped to “dhcp-relay-acl” and all DHCP packets will be switched as usual without any modifications.

Disabling 802.1x Authentication for DHCP Relay Agent

To disable the DHCP Relay Agent from sending 802.1x parameters for a particular VLAN to the DHCP server, perform this task in privileged mode:

	Task	Command
Step 1	Disable 802.1x authentication for the DHCP Relay Agent.	clear security acl map <i>acl_name</i> <i>vlan_ID</i>
Step 2	Verify the 802.1x configuration.	show dot1x

This example shows how to configure the DHCP Relay Agent to stop sending 802.1x authentication parameters for VLANs 1–3 and 20 and verify the configuration:

```
Console> (enable) clear security acl map dhcp_relay 1-3,20
Successfully cleared mapping between ACL dhcp_relay and VLAN 1.
Successfully cleared mapping between ACL dhcp_relay and VLAN 2.
Successfully cleared mapping between ACL dhcp_relay and VLAN 3.
Successfully cleared mapping between ACL dhcp_relay and VLAN 20.
```

Configuring an 802.1x Guest VLAN

You configure a guest VLAN globally. Typically, guest VLANs support minimal services and provide minimal network access. Hosts are assigned to the guest VLAN only when the **set port dot1x mod/port port-control auto** command option is used. If you change the **set port dot1x mod/port port-control** command option from **auto** to **force-authorized** or **force-unauthorized**, the host is removed from the guest VLAN and added back to the port VLAN. A VLAN does not have to be active to be configured as a guest VLAN, but it must be active before a host can use it.

To configure a VLAN as an 802.1x guest VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Configure an active VLAN as an 802.1x guest VLAN.	set port dot1x mod/port guest-vlan vlan
Step 2	Verify the 802.1x configuration.	show dot1x

This example shows how to configure VLAN 200 as an 802.1x guest VLAN on port 2/2:

```

Console> (enable) set port dot1x 2/2 guest-vlan 200
Port 2/2 Guest Vlan is set to 100
Console> (enable)Console> (enable) show dot1x
PAE Capability           Authenticator Only
Protocol Version         1
system-auth-control      enabled
max-req                  2
quiet-period             60 seconds
re-authperiod            3600 seconds
server-timeout           30 seconds
supp-timeout             30 seconds
tx-period                 30 seconds
guest-vlan                200
Console> (enable)

```

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**
- **show cam static**

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
max-req                 2
quiet-period            60 seconds
re-authperiod           3600 seconds
server-timeout          30 seconds
supp-timeout            30 seconds
tx-period               30 seconds
Dhcp-relay-agent enabled vlan(s) 1-3, 20
Console> (enable) (DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

```

To display 802.1x authenticated MAC addresses, perform this task in normal mode:

Task	Command
Display 802.1x authenticated MAC addresses.	show cam static

This example shows how to display 802.1x authenticated MAC addresses. In this example, both 802.1x and port security are enabled:

```

Console> (enable) show cam static 8/17
* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry

VLAN  Dest MAC/Route Des      [CoS]  Destination Ports or VCs / [Protocol Type]
-----
12     00-40-ca-13-ae-bf $          8/17
17     00-30-94-c2-c3-c1 X          8/17
Total Matching CAM Entries Displayed =2
Console> (enable)

```

