



# CHAPTER 40

## Configuring 802.1X Authentication

---

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



**Note**

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

---



**Note**

For information on configuring MAC address authentication bypass, see [Chapter 41, “Configuring MAC Authentication Bypass.”](#)

---



**Note**

For information on using port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses that are specified for that port, see [Chapter 38, “Configuring Port Security.”](#) That chapter also provides information on using port security to filter the traffic that is destined to or received from a specific host that is based on the host MAC address.

---



**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 39, “Configuring the Switch Access Using AAA.”](#)

---



**Note**

For information on configuring Network Admission Control, see [Chapter 44, “Configuring Network Admission Control.”](#)

---



**Note**

For information on configuring network admission control, see [Chapter 44, “Configuring Network Admission Control.”](#)

---

This chapter consists of these sections:

- [Understanding How 802.1X Authentication Works, page 40-2](#)
- [Default Authentication Configuration, page 40-11](#)
- [Authentication Configuration Guidelines, page 40-12](#)

- [Configuring 802.1X Authentication on the Switch, page 40-13](#)

## Understanding How 802.1X Authentication Works

802.1X 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. You can restrict the traffic in both directions, or you can restrict just the incoming traffic.

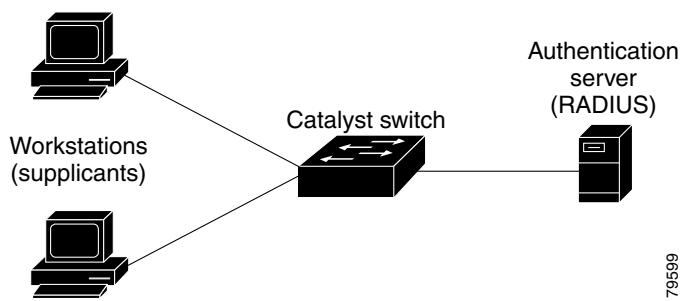
These sections provide the following information:

- [Device Roles, page 40-2](#)
- [Authentication Initiation and Message Exchange, page 40-3](#)
- [Ports in Authorized and Unauthorized States, page 40-4](#)
- [Authentication Server, page 40-6](#)
- [802.1X Parameters Configurable on the Switch, page 40-6](#)
- [Understanding How 802.1X VLAN Assignments Using a RADIUS Server Work, page 40-7](#)
- [Understanding How 802.1X Authentication with DHCP Works, page 40-8](#)
- [Understanding How 802.1X Authentication on Ports Configured for Auxiliary VLAN Traffic Works, page 40-8](#)
- [Understanding How 802.1X Authentication for the Guest VLAN Works, page 40-9](#)
- [Understanding How 802.1X Authentication with Port Security Works, page 40-10](#)
- [Understanding How 802.1X Authentication with ARP Traffic Inspection Works, page 40-11](#)

## Device Roles

With 802.1X port-based authentication, the devices in the network have specific roles. (See [Figure 40-1](#).)

**Figure 40-1** 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** 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 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 if 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 the 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 the 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.

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



**Note**

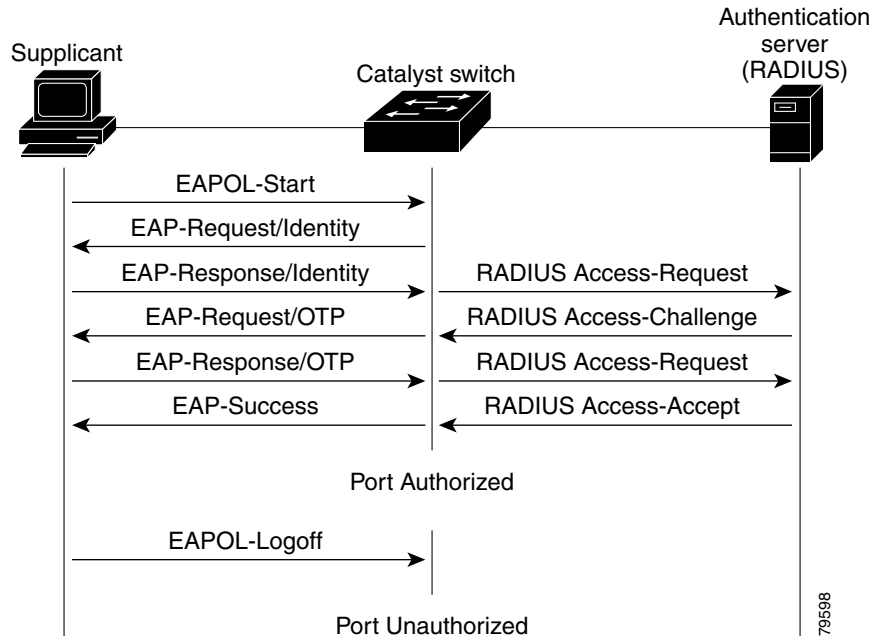
If 802.1X is not enabled or supported on the network access device, any of the EAPOL frames from the host are dropped. If the host does not receive an EAP-request/identity frame after three attempts to start authentication, the host transmits the frames as if the port is in the authorized state. A port 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 40-4.

When the host supplies its identity, the switch acts as the intermediary, passing the 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 40-4.

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

Figure 40-2 shows a message exchange that is initiated by the host using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 40-2 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 the ingress and egress traffic except for the 802.1X protocol packets. When a host is successfully authenticated, the port transitions to the *authorized* state, which allows 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 setting is the default.
- **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 the 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 the 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 40-1 defines the 802.1X terms.

**Table 40-1 802.1X Terminology**

Term	Definition
Authenticator PAE <sup>1</sup>	(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 <sup>2</sup>	Encapsulated EAP messages that can be handled directly by a LAN MAC service.

**Table 40-1 802.1X Terminology (continued)**

Term	Definition
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	Port access entity protocol object that is associated with a specific system port.
PDU	Protocol data unit.
RADIUS	Remote Access Dial-In User Service.
Supplicant <sup>3</sup> PAE	Entity that requests access to the LAN/switch services and responds to the 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. 802.1X uses the term *supplicant* for *client* or *host*. This publication uses *host* instead of *supplicant* because *host* is used in the Catalyst 6500 series CLI syntax.

## Authentication Server

The frames that are exchanged between the authenticator and the authentication server are dependent on the authentication mechanism, so they are not defined by 802.1X. You can use other protocols, but we recommend that you use RADIUS for authentication, particularly when the authentication server is located remotely, because RADIUS has extensions that support the 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 the host
- Specify the automatic host reauthentication time interval
- Specify the port shutdown timeout period after a security violation
- Enable or disable automatic host reauthentication

## Understanding How 802.1X VLAN Assignments Using a RADIUS Server Work

In the 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 the guest users in a VLAN with limited access to the network.

The 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. The 802.1X port behavior with the VLAN assignment feature is 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 you enable the multiple hosts option on an 802.1X port, all the 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 the Enhanced Address Recognition Logic (EARL) entries are cleared for the 802.1X ports.
- When an 802.1X-configured module comes up, all the 802.1X ports are configured in the 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 these three RFC 2868 attributes 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)

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.

## Understanding How 802.1X Authentication with DHCP Works

The 802.1X authentication support for the Dynamic Host Configuration Protocol (DHCP) allows the DHCP server to assign the IP addresses to the different classes of end users by adding the authenticated user identity into the DHCP discovery process. This feature allows you to secure the IP addresses given to the end users for accounting purposes and to grant the services that are based on the 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 discovery process so that the different addresses can be assigned to the different classes of users.

After the successful 802.1X authentications between the supplicant and the RADIUS server, the switch puts the port in the forwarding state and stores the attributes that 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 the 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 that 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 the 802.1X hosts on multiple ports.

## Understanding How 802.1X Authentication on Ports Configured for Auxiliary VLAN Traffic Works

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.

The ports that are configured for 802.1X authentication and an auxiliary VLAN must be in single-host authentication mode to forward the auxiliary VLAN-tagged packets from an IP phone. Because the IP phones do not have host PAE capability, when the 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 the traffic from the host PAE behind the IP phone is 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 the traffic from the new host PAE is forwarded after authentication.

---

## Understanding How 802.1X Authentication for the Guest VLAN Works

This section describes the 802.1X authentication for the guest VLANs.

A guest VLAN enables the non-802.1X capable hosts to access the networks that use 802.1X authentication. You can use the guest VLANs while you are upgrading your system to support the 802.1X authentication.

When you configure a VLAN as an 802.1X guest VLAN, all the non-802.1X capable hosts are put in this VLAN. You can configure any VLAN (except for the 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.

**Note**

In software release 8.6(1) and later releases, a private VLAN and a secondary VLAN can be configured as the guest VLAN. For more information, see the [“Configuring 802.1X Authentication with Private VLANs” section on page 40-41](#).

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.

The guest VLANs are supported in both single-authentication mode and multiple-host mode.

**Note**

Contrast the guest VLAN feature with the authentication failure VLAN feature. On a traditional 802.1X port, the switch does not provide access to the network until the supplicant that is connected to the port is authenticated by verifying its identity information with an authentication server. With an authentication failure VLAN, you can configure the authentication failure VLAN on a per-port basis and after three failed 802.1X authentication attempts by the supplicant, the port is moved to the authentication failure VLAN where the supplicant can access the network.

An authentication failure VLAN is independent of the guest VLAN. However, the guest VLAN can be the same VLAN as the authentication failure VLAN. If you do not want to differentiate between the non-802.1X capable hosts and the authentication failed hosts, you may configure both hosts to the same VLAN (either a guest VLAN or an authentication failure VLAN).

For more information, see the [“Configuring the Authentication Failure VLAN” section on page 40-38](#).

## Usage Guidelines for 802.1X Authentication with the Guest VLANs on Windows-XP Hosts

This section describes the usage guidelines for configuring 802.1X authentication with the guest VLANs on Windows-XP hosts:

- If a guest VLAN is enabled on a port, that port cannot be configured as a unidirectional port, and conversely, a unidirectional port cannot be configured in a guest VLAN.
- If the host fails to respond to the authenticator, the port remains in the connecting state for 180 seconds. After this time, the login/password window does not appear on the host. The workaround is to have the user unplug and then reconnect the network interface cable.

- The hosts that respond with an incorrect login/password fail authentication are not put in the guest VLAN. The first time that a host fails authentication, the quiet-period timer starts and no activity occurs 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 occurs for the duration of the quiet-period timer. The host is presented with the login/password window a third time. If the host fails the third time, the port is put in the connecting and unauthorized states. The workaround to this problem is to have the user unplug and then reconnect the network interface cable.
- If a host does not respond to the username and password authentication requests from the Authenticator PAE, it is placed in a guest VLAN.

**Note**


---

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

---

## Understanding How 802.1X Authentication with Port Security Works

802.1X authentication is compatible with the port security feature (for more information, see Chapter 38, “[Configuring Port Security](#)”). If you enable port security for only one MAC address on a specific port, only that MAC address authenticates through a RADIUS server. The users that are 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**


---

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. The host is authenticated first and is then secured by port security.

---

You can enable port security for any 802.1X mode (single-authentication mode, multiple-host mode, or multiple-authentication mode). 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 mode and multiple-host mode. 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 fewer addresses 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.

In 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.

## Understanding How 802.1X Authentication with ARP Traffic Inspection Works



### Note

This feature is available only with Supervisor Engine 2 with PFC2, Supervisor Engine 720 with PFC3A/PFC3B/PFC3BXL, and Supervisor Engine 32 with PFC3B/PFC3BXL.

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 complements 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.

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 the 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 the 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 the unsolicited ARP replies (or the gratuitous ARP packets) to the 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 the 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.

To configure ARP traffic inspection, see the “[Inspecting ARP Traffic](#)” section on page 15-30.

## Default Authentication Configuration

[Table 40-2](#) shows the default 802.1X authentication configuration.

**Table 40-2** 802.1X Authentication Default Configuration

Feature	Default Value
PAE Capability	Authenticator only
Protocol Version	1
802.1X port control	Force-authorized
802.1X multiple hosts	Disabled
802.1X system authentication control	Enabled
802.1X quiet period time	60 seconds

**Table 40-2 802.1X Authentication Default Configuration (continued)**

Feature	Default Value
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 the host	2
802.1X automatic host reauthentication time	3600 seconds
802.1X automatic authenticator reauthentication of the host	Disabled
802.1X shutdown timeout period	300 seconds
802.1X RADIUS accounting	Disabled
802.1X RADIUS VLAN assignment	Enabled
802.1X RADIUS keepalive state	Enabled

## 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 the 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 trunking 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 dynamic VLAN on that port. You cannot enable dynamic VLAN on an 802.1X port.
- You cannot enable 802.1X on a channeling port until you turn off channeling 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. We recommend that you do not enable the multiple-host option on an 802.1X-enabled auxiliary port.
- 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.
- On an 802.1X-enabled port, an administratively configured VLAN cannot be equal to an auxiliary VLAN.

- The private VLANs and 802.1X configurations are mutually exclusive of one another.



**Note** Software release 8.6(1) and later releases provide support for configuring 802.1X with private VLANs. For more information, see the “[Configuring 802.1X Authentication with Private VLANs](#)” section on page 40-41.

- With a PFC3A/PFC3B/PFC3BXL, you can use the **set rate-limit l2port-security** command to enable, disable, or set the 802.1X port security rate limiters globally on the switch. For more information on configuring rate limiting, see the “[Configuring Layer 2 PDU Rate Limiting on the Switch](#)” section on page 7-61.

## 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 “[Understanding How 802.1X VLAN Assignments Using a RADIUS Server Work](#)” section on page 40-7.

- [Enabling 802.1X Authentication Globally](#), page 40-14
- [Disabling 802.1X Authentication Globally](#), page 40-14
- [Enabling 802.1X Authentication for Individual Ports](#), page 40-15
- [Enabling 802.1X with Inaccessible Authentication Bypass](#), page 40-15
- [Enabling Multiple 802.1X Authentications](#), page 40-16
- [Setting and Enabling Automatic Reauthentication of the Host](#), page 40-17
- [Manually Reauthenticating the Host](#), page 40-18
- [Enabling Multiple Hosts](#), page 40-18
- [Disabling Multiple Hosts](#), page 40-19
- [Setting the Quiet Period](#), page 40-19
- [Setting the Shutdown Timeout Period](#), page 40-19
- [Setting the Authenticator-to-Host Retransmission Time for EAP-Request/Identity Frames](#), page 40-20
- [Setting the Back-End Authenticator-to-Host Retransmission Time for the EAP-Request Frames](#), page 40-20
- [Setting the Back-End Authenticator-to-Authentication-Server Retransmission Time for the Transport Layer Packets](#), page 40-21
- [Setting the Back-End Authenticator-to-Host Frame-Retransmission Number](#), page 40-21
- [Setting the Critical Recovery Delay for an Authentication Feature](#), page 40-21
- [Resetting the 802.1X Configuration Parameters to the Default Values](#), page 40-22
- [Enabling 802.1X Authentication for the DHCP Relay Agent](#), page 40-23
- [Disabling 802.1X Authentication for the DHCP Relay Agent](#), page 40-24
- [Adding Hosts to an 802.1X Guest VLAN](#), page 40-24

- [Configuring an 802.1X Unidirectional Controlled Port](#), page 40-25
- [Configuring 802.1X with ACL Assignments](#), page 40-26
- [Configuring 802.1X User Distribution](#), page 40-32
- [Enabling and Disabling 802.1X RADIUS Accounting and Tracking](#), page 40-34
- [Enabling and Disabling RADIUS Keepalive](#), page 40-36
- [Configuring the Authenticated Identity-to-Port Description Mappings](#), page 40-37
- [Configuring the DNS Resolution for a RADIUS Server Configuration](#), page 40-37
- [Configuring the Authentication Failure VLAN](#), page 40-38
- [Configuring a RADIUS Server Failover](#), page 40-40
- [Configuring 802.1X Authentication with Private VLANs](#), page 40-41
- [Using the show Commands](#), page 40-47

## Enabling 802.1X Authentication Globally

You must enable 802.1X authentication for the entire system before you can configure it for the individual ports. After you globally enable 802.1X authentication, you can configure the individual ports for 802.1X authentication if the port meets the specific requirements that are required by 802.1X. To enable 802.1X authentication for the individual ports, see the [“Enabling 802.1X Authentication for Individual Ports”](#) section on page 40-15.

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

Task	Command
Globally enable 802.1X authentication.	<b>set dot1x system-auth-control enable</b>

This example shows how to enable 802.1X authentication globally:

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

## Disabling 802.1X Authentication 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 disable 802.1X authentication globally, perform this task in privileged mode:

Task	Command
Globally disable 802.1X authentication.	<b>set dot1x system-auth-control disable</b>

This example shows how to disable 802.1X authentication globally:

```
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 the individual ports. To enable 802.1X authentication globally, see the [“Enabling 802.1X Authentication Globally”](#) section on page 40-14.



### Note

You must specify at least one RADIUS server before you can enable 802.1X authentication on the switch. For more information, 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.	<b>set port dot1x mod/port port-control auto</b>
Step 2	Verify the 802.1X configuration.	<b>show port dot1x mod/port</b>

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

```

Console> (enable) set port dot1x 3/1 port-control auto
Port 3/1 dot1x port-control is set to auto.
Trunking disabled for port 3/1 due to Dot1x feature.
Spanntree port fast start option enabled for port 3/1.
Console> (enable) show port dot1x 3/1
Port  Auth-State      BEnd-State  Port-Control  Port-Status
-----
 3/1  connecting         idle        auto          unauthorized

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
 3/1  SingleAuth    disabled           disabled          Both    Both
Console> (enable)

```



### Note

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

## Enabling 802.1X with Inaccessible Authentication Bypass

You can enable 802.1X inaccessible authentication bypass on a per-port basis. This feature allows you to specify a port as critical. When a port is specified as a critical port, 802.1X attempts to authenticate the port in the normal way. If attempts to reach the authentication server fail, the port is still given access to the network in the administratively configured VLAN or the port’s native VLAN. You can configure a port as critical only if it is in single-authentication mode.

After a critical port obtains access to the network, if the authentication server becomes available, the critical port returns to the unauthorized state, the normal authentication process restarts, and the critical port moves into the RADIUS server-specified VLAN after the port is authenticated. At this point, you must initialize the port manually using the **set port dot1x mod/port initialize** command.

If the authentication server goes down after a host has already been authenticated through the normal authentication process, the switch checks if the port is a critical port. If the switch determines that the port is a critical port, the normal reauthentication process is temporarily disabled for the port and the port is given network access until the authentication server becomes active and restarts the authentication process.

To specify a port as a critical port, perform this task in privileged mode:

	Task	Command
Step 1	Specify a port as a critical port.	<b>set port dot1x mod/port critical {enable   disable}</b>
Step 2	Verify the 802.1X configuration.	<b>show port dot1x mod/port</b>

This example shows how to specify a port as a critical port:

```
Console> (enable) set port dot1x 5/48 critical enable
Port 5/48 critical-port option is enabled
Console> (enable)
```

This example shows how to verify the 802.1X configuration:

```
Console> (enable) show port dot1x 5/48
Port  Auth-State      BEnd-State  Port-Control      Port-Status
-----
5/48  -                  -           force-authorized  -

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
5/48  SingleAuth    disabled          disabled          Both      -

Port  Posture-Token  Critical  Termination action  Session-timeout
-----
5/48  -              YES      -                  -
Console> (enable)
```

## Enabling Multiple 802.1X Authentications

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

- The traffic from the non-802.1X hosts on multiple authenticated ports is blocked.
- You cannot enable a guest VLAN on multiple authenticated ports.
- You cannot enable multiple authentication on a MVAP.
- Multiple authenticated ports go into the port VLAN and will not go into a RADIUS-assigned VLAN.
- You need to enable port security on a port before you can enable multiple authentications on the port.
- You cannot disable port security on a multiple authenticated port.
- The port security timers are used on multiple authenticated ports. The 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 authentications on a specific port.	<b>set port dot1x <i>mod/port</i> multiple-authentication {enable   disable}</b>
Step 2	Verify the 802.1X configuration.	<b>show port dot1x <i>mod/port</i></b>

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

```

Console> (enable) set port dot1x 3/1 multiple-authentication enable
PortSecurity should be enabled on port 3/1, before enabling Multiple-authentication
Port Security not enabled on 3/1.
Console> (enable) set port security 3/1 enable
Port 3/1 security enabled.
Console> (enable) set port dot1x 3/1 multiple-authentication enable
Port 3/1 Multiple-authentication option enabled
Console> (enable) show port dot1x 3/1
Port  Auth-State          BEnd-State  Port-Control  Port-Status
-----
 3/1  connecting            idle        auto          unauthorized

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
 3/1  MultiAuth     disabled           disabled          Both    Both
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 3600 seconds (the valid values are from 1–65535 seconds).

You can enable automatic 802.1X host reauthentication for the 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 40-18.

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.	<b>set dot1x re-authperiod <i>seconds</i></b>
Step 2	Enable reauthentication.	<b>set port dot1x <i>mod/port</i> re-authentication enable</b>
Step 3	Verify the 802.1X configuration.	<b>show port dot1x <i>mod/port</i></b>

This example shows how to set automatic reauthentication to 7200 seconds, enable 802.1X reauthentication on port 3/1, and verify the configuration:

```

Console> (enable) set dot1x re-authperiod 7200
dot1x re-authperiod set to 7200 seconds
Console> (enable) set port dot1x 3/1 re-authentication enable
Port 3/1 Dot1x re-authentication enabled.
Console> (enable) show port dot1x 3/1
Port  Auth-State      BEnd-State  Port-Control      Port-Status
-----
 3/1  connecting         idle        auto              unauthorized

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
 3/1  MultiAuth     enabled           disabled          Both    Both
Console> (enable)

```

## 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 40-17.

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.	<b>set port dot1x <i>mod/port</i> re-authenticate</b>

This example shows how to manually reauthenticate the host that is connected to port 1 on module 3:

```

Console> (enable) set port dot1x 3/1 re-authenticate
Port 3/1 re-authenticating...
dot1x re-authentication successful...
dot1x port 3/1 authorized.
Console> (enable)

```

## 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 the 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 access for multiple hosts on a specific port, perform this task in privileged mode:

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

This example shows how to enable access for multiple hosts on port 1 on module 3:

```
Console> (enable) set port dot1x 3/1 multiple-host enable
Port 3/1 Multiple-host option enabled.
Console> (enable)
```

## Disabling Multiple Hosts

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

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

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

This example shows how to disable access for multiple hosts on port 1 on module 3:

```
Console> (enable) set port dot1x 3/1 multiple-host disable
Port 3/1 Multiple-host option disabled.
Console> (enable)
```

## 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.	<b>set dot1x quiet-period <i>seconds</i></b>

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.
Console> (enable)
```

## Setting the Shutdown Timeout Period

If a port is shut down because of a security violation, you must either manually reenable 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.	<b>set dot1x shutdown-timeout <i>1- 65535 seconds</i></b>

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 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.	<b>set dot1x tx-period</b> <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.
Console> (enable)
```

## Setting the Back-End Authenticator-to-Host Retransmission Time for the 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.	<b>set dot1x supp-timeout</b> <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.
Console> (enable)
```

## Setting the Back-End Authenticator-to-Authentication-Server Retransmission Time for the 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 the transport layer packets.	<b>set dot1x server-timeout</b> <i>seconds</i>

This example shows how to set the value for the retransmission time for the 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.
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.	<b>set dot1x max-req</b> <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.
Console> (enable)
```

## Setting the Critical Recovery Delay for an Authentication Feature

You can set the critical recovery delay for each authentication feature. By default, critical recovery delay is disabled. The critical recovery delay can be set between 1–10000 milliseconds. Ports enabled with the critical recovery delay feature will be moved to the “critical” state when the RADIUS server is not

available to authenticate. The ports moved to critical state are initialized when the RADIUS server comes online and the RADIUS auto-initialization feature is enabled. During the initialization process, the ports that were moved to the critical state are initialized after the configured critical recovery delay interval.

For example, if there are 10 ports enabled with dot1x and moved to the critical state, the ports are initialized when the RADIUS server comes online. If you configure a delay of 10 milliseconds, the initialization for each port is delayed by 10 milliseconds before the initialization process begins. After each 10-millisecond period is completed, the next port initializes until all the ports have gone through the initialization process.

Task	Command
Set the critical recovery delay feature.	<b>set [dot1x   mac-auth-bypass   eou   web-auth] critical-recovery-delay <i>time</i></b>

This example shows how to set the critical recovery delay to 10 milliseconds for dot1x:

```
Console> (enable) set dot1x critical-recovery-delay 10
Dot1x critical recovery delay set to 10 milliseconds.
Console> (enable)
```

## 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
<b>Step 1</b>	Reset the 802.1X configuration parameters to the default values and globally disable 802.1X.	<b>clear dot1x config</b>
<b>Step 2</b>	Verify the 802.1X configuration.	<b>show dot1x</b>

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              45 seconds
radius-accounting         disabled
radius-vlan-assignment   enabled
radius-keepalive state   enabled
re-authperiod            7200 seconds
server-timeout            30 seconds
shutdown-timeout         300 seconds
supp-timeout              30 seconds
tx-period                 30 seconds
```

```
Console> (enable)
```

## 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:



### Note

The management VLAN (the VLAN that is configured on the sc0 or sc1 interfaces) cannot be mapped to an ACL that has a dot1x-dhcp ACE. You cannot use the **clear config interface** command when VLAN 1 or VLAN 2 is mapped to an ACL that has a dot1x-dhcp ACE.

	Task	Command
Step 1	Enable 802.1X authentication for the DHCP Relay Agent.  <b>Note</b> 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.	<b>set security acl ip <i>acl_name</i> permit dot1x-dhcp</b>
Step 2	Verify the 802.1X configuration.	<b>show dot1x</b>

This example shows how to create an ACL entry for the 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 how to configure the ACL to allow other traffic than DHCP on an existing ACL entry:

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

## Disabling 802.1X Authentication for the DHCP Relay Agent

To disable the DHCP Relay Agent from sending the 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.	<b>clear security acl map dhcp_relay <i>vlan_ID</i></b>
Step 2	Verify the 802.1X configuration.	<b>show dot1x</b>

This example shows how to configure the DHCP Relay Agent to stop sending the 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.
```

## Adding Hosts to an 802.1X Guest VLAN

Typically, the guest VLANs support minimal services and provide minimal network access. The hosts can be added 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.

To add a port to 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.	<b>set port dot1x mod/port guest-vlan {<i>vlan</i>   none}</b>
Step 2	Verify the per-port 802.1X guest VLAN configuration.	<b>show port dot1x guest-vlan</b>

This example shows how to add port 3/1 to 802.1X guest VLAN 200:

```
Console> (enable) set port dot1x 3/1 guest-vlan 200
Port 3/1 is Multiple-authentication enabled, guest-vlan can not be enabled
Console> (enable) set port dot1x 3/1 multiple-authentication disable
Port 3/1 Multiple-authentication option disabled
Console> (enable) set port dot1x 3/1 guest-vlan 200
Port 3/1 Guest Vlan is set to 200
Console> (enable) show port dot1x guest-vlan
Guest-Vlan   Status   Mod/Ports
-----
200          active   3/1
none         none     2/1-2,3/2-48,8/1-8
Console> (enable)
```

This example shows how to remove the port from the guest VLAN:

```
Console> (enable) set port dot1x 3/1 guest-vlan none  
Port 3/1 Guest Vlan is cleared  
Console> (enable)
```

## Configuring an 802.1X Unidirectional Controlled Port

802.1X allows you to use wake-on LAN technology (also referred to as remote wake-up) to perform the unattended system backups or software upgrades on the hosts that are attached to the switch.

When you configure a unidirectional controlled port, the port allows outbound-only traffic prior to host authentication. This behavior enables a management station to send the wake-on LAN frames to selected hosts that trigger the host to power up and boot, authenticate, and then perform the unattended operation.



### Note

The wake-on LAN technology requires specific hardware for the host that is outside the scope of this publication.

Prior to software release 8.3(1), the 802.1X bridge ports were configured by default to a bidirectional state where the control was exerted on protocol exchanges in both directions on the unauthorized ports. With the unidirectional controlled port feature, you can configure the 802.1X-capable ports to be in unidirectional (**in** keyword) or bidirectional (**both** keyword) states using the **set port dot1x mod/port port-control-direction** command.

## Unidirectional State

When you configure a port as a unidirectional port (**in** keyword) and set the port to **auto** using the **set port dot1x mod/port port-control auto** command, the bridge port is moved into the spanning-tree forwarding state where all the traffic to the port is redirected to the supervisor engine for processing. With the wake-on LAN functionality, when the connected host is in sleeping mode or a power-down state, the host does not exchange the traffic with any other devices in the network. The hosts that are connected to the unidirectional port cannot send the traffic out into the network; they can only receive the traffic from the other devices in the network. If the unidirectional port sees any kind of incoming traffic, the port returns to the bidirectional (default) state and the spanning-tree state is moved to the blocking state where both the incoming and outgoing traffic are dropped. The authenticator system on the port moves the port into the initialize state and no traffic is allowed other than the EAPOL packet exchanges. When the port is returned to the bidirectional state, a 5-minute timer is started and if the port is not authenticated before the timer runs out, the port switches back to a unidirectional port.

## Bidirectional State

When you configure a port as a bidirectional port (**both** keyword) and set the port to **auto** using the **set port dot1x mod/port port-control auto** command, the port is access controlled in both directions. This state disables the reception of any incoming packets and the transmission of outgoing packets on the port. When the port is configured as a bidirectional port, it behaves as it did in software releases prior to release 8.3(1); the port is in the spanning-tree blocking state and the normal authentication process is followed.

## Configuration Guidelines

This section provides the guidelines for configuring 802.1X unidirectional ports:

- **Auxiliary VLANs**—To support auxiliary VLANs on a port when you configure the port as a unidirectional port, the auxiliary VLAN is moved to the spanning-tree forwarding state to ensure that the connected IP phone is operational immediately. To prevent any disturbance of the incoming traffic, initially the port VLAN is also moved to the spanning-tree forwarding state and then if any traffic is seen on the port VLAN, the port is moved to the spanning-tree blocking state to drop all additional traffic. The connected host is then requested to get authorized to send any traffic.
- **Guest VLANs**—The guest VLANs are supported only on the ports that are configured as bidirectional ports. If a guest VLAN is enabled on a port, that port cannot be configured as a unidirectional port, and conversely, a unidirectional port cannot be configured in a guest VLAN.
- **Port mode**—The port mode (single-authentication mode, multiple-host mode, or multiple-authentication mode) for a port configured as a unidirectional port must be single-authentication mode (the default port mode).

## Using the CLI to Configure an 802.1X Unidirectional or Bidirectional Port

If you specify the **in** keyword, all the incoming traffic is dropped and the outgoing traffic is allowed. If you specify the **both** keyword (the default), all the receiving traffic and transmitting traffic on the port is dropped. To configure a port as an 802.1X unidirectional port or bidirectional port, perform this task in privileged mode:

Task	Command
Configure a port as an 802.1X unidirectional port or bidirectional port.	<b>set port dot1x mod/port port-control-direction [both   in]</b>

These examples show how to set a port to unidirectional or bidirectional states and verify the configuration:

```

Console> (enable) set port dot1x 3/1 port-control-direction both
Port 3/1 Port Control Direction set to Both.
Console> (enable) set port dot1x 3/1 port-control-direction in
Port 3/1 Port Control Direction set to In.
Console> (enable) show port dot1x 3/1
Port  Auth-State      BEnd-State  Port-Control  Port-Status
-----
 3/1  connecting         idle        auto          unauthorized

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
 3/1  SingleAuth    enabled            disabled          In      Both
Console> (enable)

```

## Configuring 802.1X with ACL Assignments

These sections describe how to configure 802.1X with ACL assignments:

- [Overview, page 40-27](#)
- [802.1X with ACL Assignments Configuration Guidelines, page 40-28](#)

- [Using the CLI to Configure 802.1X with ACL Assignments, page 40-28](#)
- [Configuring 802.1X with QoS ACLs, page 40-29](#)

## Overview

When you configure 802.1X with ACL assignments, the identity-based ACLs are used to dynamically assign an access control policy to an interface that is based on the user's 802.1X authentication. This feature restricts the users to certain network segments, limits the access to the sensitive servers, and restricts the protocols and applications that may be used. This feature also allows you to provide very specific identity-based security without compromising user mobility or significantly increasing the administrative overhead.

When you configure 802.1X with ACL assignments, you eliminate the problem of creating, modifying, and removing the access control policies that are based on the IP/MAC addresses whenever the user's physical location changes in the network. This feature allows you to create the identity-based security access policies rather than the VLAN-based policies (VACLs) or the port-based policies (PACLs) without compromising user mobility. With this feature, the user does not have to rely on the network administrator to enforce the access policy changes whenever the user's physical location and/or connection to the network changes.

The new **group** *group\_name* keyword is used to classify the policy as a group. A group is a set of users (their IP addresses) to which the policy applies. Prior to this feature, if you wanted to permit the IP access to a set of users, you had to specify each user's IP address in the ACL ACE and there could only be one IP address per ACE. With this new feature, you specify a *group\_name* in the ACE, such as **set security acl ip grpacl permit ip group ip-permit-group any**, where the *ip-permit-group* is a group and all the users that are part of that group are authenticated. After a successful user authentication and after the user's IP address is obtained, if the user is part of the group, the user's IP address is added to the group and a new ACE is created and installed in the hardware (PFC). The ACL grows and shrinks dynamically upon user authentication and logoff; the ACL is dynamic and the policy is installed only for the authenticated and valid users.

When you configure 802.1X with ACL assignments, you can automatically configure the QoS ACLs and VACLs to a user once the user is authenticated. The RADIUS server sends a QoS VLAN-based ACL, QoS port-based ACL, or VACL policy name with the authentication success packet. The policy that is associated with the policy name is already configured on the switch through the CLI. The policy is converted into a set of ACEs and then installed on the switch.

You can apply the ACLs to an IP address. Because the 802.1X authentication is done on a username and can be tied to a MAC address—but the IP address is not known at the time of authentication (DHCP is started by the host only after a successful authentication)—the ACE installation occurs only after the IP address is known either through DHCP snooping or dynamic ARP inspection.

When you configure 802.1X with ACL assignments, you perform these two main configuration tasks:

- Associate and configure the group names for the users in the RADIUS server
- Configure, commit, and map the ACLs on the switch for the groups using the switch CLI

After you configure the 802.1X ACL assignments, the switch does the following:

- Authenticates the user(s)
- Uses DHCP snooping or dynamic ARP inspection to obtain the IP address of the user(s)
- Expands the ACL using the IP address(es) and programs the PFC

## 802.1X with ACL Assignments Configuration Guidelines

This section provides the guidelines for configuring 802.1X with ACL assignments:

- The port mode (single-authentication mode, multiple-host mode, or multiple-authentication mode) for a port that is configured for 802.1X with ACL assignments must be single-authentication mode (the default port mode).
- Dynamically learned IP addresses (obtained through DHCP snooping or dynamic ARP inspection) are used to expand the group name. 802.1X with ACL assignments is also supported with static IP addresses (the static IP address should also be configured in the RADIUS server).
- The groups are policy groups. An example of a policy group would be a policy such as “deny http access” that applies to a set of IP addresses.
- The user is never permanently tied to a group, and a user can be part of multiple policy groups simultaneously. If you want to define more than one policy, for example, if you want both “deny http access” and “deny ftp access,” you can define two policy groups—one policy group as “http deny” and another policy group as “ftp deny.”
- The RADIUS server can send all the policies that have to be applied to a particular user in the authentication success packet, and the user can be added to all those groups on the switch. If a policy group sent by the RADIUS server is not configured on the switch, the policy is either ignored or the port goes into the unauthorized state. If the RADIUS server sends a group ID that is not present in any ACL on the switch, authentication fails.
- With software release 8.3(1) and later releases, you can load balance the 802.1X-authenticated users that are configured under one group name by distributing them evenly between the VLANs. For more configuration information, see the “[Configuring 802.1X User Distribution](#)” section on [page 40-32](#).

## Using the CLI to Configure 802.1X with ACL Assignments



### Note

This section describes the CLI introduced in software release 8.3(1), which is used to configure 802.1X with ACL assignments. For more information on configuring the ACLs, see [Chapter 15, “Configuring Access Control.”](#)

To configure 802.1X with ACL assignments, perform this task in privileged mode:

Task	Command
Configure 802.1X with ACL assignments.	<b>set security acl ip</b> {acl_name} {permit   deny   redirect {mod_num/port_num}} [ip] {src_ip_spec   [group {group_name}]} {dest_ip_spec   [group] [precedence {precedence}]} [tos {tos}] [fragment] [capture] [log] [before {editbuffer_index}   modify {editbuffer_index}]

This example shows how to specify a group name for an 802.1X group and verify that the group was configured:

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

```
ACL commit in progress.

ACL 'grpacl' successfully committed.
Console> (enable)

Console> (enable) show dot1x group all
Group Manager Info

Current Group Count = 1

-----
Info of Group ip-permit-group
User Count = 0
Console> (enable)
```

## Configuring 802.1X with QoS ACLs

These sections describe how to configure 802.1X with QoS ACLs:

- [802.1X with QoS ACLs Configuration Guidelines, page 40-29](#)
- [802.1X with QoS ACLs Configuration Example, page 40-30](#)
- [Configuring the RADIUS Server, page 40-31](#)

The RADIUS server sends a policy name to the 802.1X client. The policy is already defined and committed on the switch. The user is able to fully utilize all existing QoS features when defining the QoS policy. The 802.1X client interacts with the QoS subsystem and applies the policy on an interface after authentication has been made. The policy is removed when the authenticated client leaves the interface. If 802.1X has attached a policy to an interface, it is still possible for you to unmap the policy directly through the switch CLI.

### 802.1X with QoS ACLs Configuration Guidelines

This section describes the guidelines for configuring 802.1X with QoS ACLs:

- If a QoS policy misconfiguration exists and 802.1X attempts to authenticate a user on an interface, the authentication will fail.
- If you misconfigure a QoS policy after 802.1X has properly authenticated the interface, authentication will fail when reauthentication is attempted on the interface with that same QoS policy.
- If multiple QoS policies are applied at the same time (input and output policies), authentication will fail if any of the QoS policies fail.
- If you apply a port-based policy and a VLAN-based policy to the same interface, the authentication will fail.
- The 802.1X security and QoS policies are applied only when an 802.1X user logs in. If you change the 802.1X security and/or QoS policy on the switch or the RADIUS server, the changes are not applied until the 802.1X user reauthenticates. If reauthentication is enabled (nondefault), the policy will take effect usually within one hour. If reauthentication is disabled (default), the policy changes will not take effect until each 802.1X user logs out and logs back in.
- The existing QoS commands are used to create and show the QoS policy information. The commands include but are not limited to the **set qos enable**, **set qos acl**, and **commit qos acl** commands. Scheduling commands and port-based QoS commands may also be used to build the dynamic QoS policy.

- After you define a QoS policy on the switch, you should map the policy to a VLAN or port (using the **set qos acl map** command) and verify that the policy mapping succeeds. After verification, clear the ACL mapping and configure 802.1X on the interface.

**Note**

Be careful when you name the QoS ACL. The QoS ACL name must match the policy name specified on the RADIUS server.

### 802.1X with QoS ACLs Configuration Example

In the following example, QoS is enabled and an 802.1X QoS policy (Dot1xDscp5Policy) is created. The policy is then committed. The same policy name (Dot1xDscp5Policy) is then configured on the RADIUS server. After a period of time, you can see that the policy is applied to port 3/1 after 802.1X has authenticated a client and applied the policy. You can see that the policy mapping is not found in the configuration (config) display of the mapping command: it is found only in the run-time configuration.

The AV-pairs at the RADIUS server require the following input—qos:inpacl=Dot1xDscp5Policy. After supplicant authentication on port 3/1, the QoS run-time mapping to port 3/1 occurs.

The other options for the AV-pairs are as follows—qos:invacl=<policy-name> and qos:outpacl=<policy-name>.

If the policy name in the AV-pairs does not match a policy name in the switch, the supplicant is not authenticated.

```
Console> (enable) set qos enable
QoS is enabled.
Console> (enable) set qos acl ip Dot1xDscp5Policy dscp 5 any
Dot1xDscp5Policy editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit qos acl all
```

QoS ACL 'Dot1xDscp5Policy' successfully committed.

```
Console> (enable) show qos acl map config Dot1xDscp5Policy
```

QoS ACL mappings on input side:

ACL name	Type	Vlans
Dot1xDscp5Policy	IP	
ACL name	Type	Ports
Dot1xDscp5Policy	IP	

QoS ACL mappings on output side:

ACL name	Type	Vlans
Dot1xDscp5Policy	IP	

```
Console> (enable)
```

<<< Dot1x Authenticates a client on 3/1 and applies Dot1xDscp5Policy >>>

```
Console> (enable) show qos acl map runtime Dot1xDscp5Policy
```

QoS ACL mappings on input side:

ACL name	Type	Vlans
Dot1xDscp5Policy	IP	
ACL name	Type	Ports
Dot1xDscp5Policy	IP	3/1

QoS ACL mappings on output side:

ACL name	Type	Vlans
Dot1xDscp5Policy	IP	

```
Console> (enable) show qos acl map config Dot1xDscp5Policy
```

```

QoS ACL mappings on input side:
ACL name                               Type Vlans
-----
Dot1xDscp5Policy                        IP
ACL name                               Type Ports
-----
Dot1xDscp5Policy                        IP
QoS ACL mappings on output side:
ACL name                               Type Vlans
-----
Dot1xDscp5Policy                        IP
Console> (enable)

```

This example shows that the dynamic QoS policy information is displayed using the **show qos acl map** command. When you use the **runtime** keyword, you can see which dynamic policies have been applied to which interfaces. The **config** keyword does not show the dynamic QoS policy mapping.

```

Console> (enable) show qos acl map config Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                               Type Vlans
-----
Dot1xDscp5Policy                        IP
ACL name                               Type Ports
-----
Dot1xDscp5Policy                        IP
QoS ACL mappings on output side:
ACL name                               Type Vlans
-----
Dot1xDscp5Policy                        IP
Console> (enable) show qos acl map runtime Dot1xDscp5Policy
QoS ACL mappings on input side:
ACL name                               Type Vlans
-----
Dot1xDscp5Policy                        IP
ACL name                               Type Ports
-----
Dot1xDscp5Policy                        IP 3/1
QoS ACL mappings on output side:
ACL name                               Type Vlans
-----
Dot1xDscp5Policy                        IP
Console> (enable)

```

## Configuring the RADIUS Server

Using Cisco Secure Access Control Server (ACS) 3.x or higher, you need to configure the QoS policy name associated with an authenticated client. To configure the RADIUS server, perform these steps from the ACS home page:

- 
- Step 1** Select **network configuration**.
  - Step 2** Click on the NAS IP on which to turn on the RADIUS IOS/PIX style of attributes. You will get the Authenticate Using field.
  - Step 3** Select the **IOS/PIX** option and submit.
  - Step 4** Select **interface config**.
  - Step 5** Select **RADIUS (IOS/PIX)**.
  - Step 6** Check both boxes before the AV-pair option. The first option itself is AV-pair.

The AV-pair box appears for every user. Check the box and then type the AV-pair strings in the window. The strings in this case represent the QoS policy name that you wish to associate with each user. If you are sending multiple AV-pair strings, you need to separate them with a new line so that each AV-pair is sent as a different 26/9/1 attribute.

## Configuring 802.1X User Distribution

When you configure 802.1X user distribution, you can distribute the users that have the same group name across multiple VLANs. Before software release 8.3(1), the RADIUS VLAN assignment feature that was supported by 802.1X took the VLAN number that was obtained from the RADIUS server and added all the users to that VLAN. With software release 8.3(1) and later releases, you can load balance the 802.1X-authenticated users that are configured under one group name by distributing them evenly between the VLANs.

Use these two methods to load balance the users between the different VLANs. The VLANs are either supplied by the RADIUS server or configured under a VLAN group name through the switch CLI:

- Configure the RADIUS server to send more than one VLAN name for a user. The multiple VLAN names can be sent as part of the response to the user. The 802.1X user distribution tracks all the users in a particular VLAN and achieves load balancing by moving the authorized user to the least populated VLAN.
- Configure the RADIUS server to send a VLAN group name for a user. The VLAN group name can be sent as part of the response to the user. The selected VLAN group name is searched among the VLAN group names that you configured using the Catalyst CLI (see the [“Using the CLI to Configure 802.1X User Distribution”](#) section on page 40-33). If the VLAN group name is found, the corresponding VLANs that are configured under this VLAN group name are searched to find the least populated VLAN and load balancing is achieved by moving the corresponding authorized user to that VLAN.

## 802.1X User Distribution Configuration Guidelines

This section provides the guidelines for configuring the 802.1X user distribution feature:

- Ensure that at least one VLAN is mapped to the VLAN group.
- You can map more than one VLAN to a VLAN group.
- You can modify the VLAN group by adding or deleting a VLAN.
- When you clear an existing VLAN from the VLAN group name, none of the ports that are authenticated in the VLAN are cleared but the mappings are removed from the existing VLAN group.
- If you clear the last VLAN from the VLAN group name, the VLAN group is deleted.
- You can clear a VLAN group even when the active VLANs are mapped to the group. When you clear a VLAN group, none of the ports or users that are in the authenticated state in any VLAN within the group are cleared, but the VLAN mappings to the VLAN group are cleared.
- If you enter the **set dot1x radius-vlan-assignment disable** command, the VLAN information that is sent from the RADIUS server is ignored and the port stays in the NVRAM-configured VLAN. This command is used to enable or disable the VLAN assignment feature globally. When the command is enabled, the switch uses the tunnel attributes to extract the VLAN name in the RADIUS Access-Accept message. The command is enabled by default.

## Using the CLI to Configure 802.1X User Distribution

To configure a VLAN group and map a VLAN to it, perform these tasks in privileged mode:

Task	Command
Configure a VLAN group and map a single VLAN or a range of VLANs to it.	<b>set dot1x vlan-group</b> { <i>vlan-group-name</i> } { <i>vlangs</i> }
Verify the configuration.	<b>show dot1x vlan-group</b> [all   { <i>vlan-group-name</i> }]
Clear the VLAN group configuration or elements of the VLAN group configuration.	<b>clear dot1x vlan-group</b> [all { <i>vlan-group-name</i> } [ <i>vlangs</i> ]]

This example shows how to configure the VLAN groups, map the VLANs to the groups, and verify that the VLAN groups were configured and mapped to the specified VLANs:

```

Console> (enable) set dot1x vlan-group eng-dept 10
Vlan group name eng-dept is successfully configured and mapped to vlan 10
Console> (enable) set dot1x vlan-group hr-dept 20
Vlan group name hr-dept is successfully configured and mapped to vlan 20
Console> (enable) show dot1x vlan-group eng-dept
Group Name                Vlans Mapped
-----
eng-dept                   10
Console> (enable) show dot1x vlan-group all
Group Name                Vlans Mapped
-----
eng-dept                   10
hr-dept                    20
Console> (enable)

```

This example shows how to add a VLAN to an existing VLAN group and verify that the VLAN was added:

```

Console> (enable) set dot1x vlan-group eng-dept 30
Vlan 30 is successfully mapped to vlan group eng-dept.
Console> (enable) show dot1x vlan-group eng-dept
Group Name                Vlans Mapped
-----
eng-dept                   10,30
Console> (enable)

```

This example shows how to clear a VLAN from a VLAN group:

```

Console> (enable) clear dot1x vlan-group eng-dept 10
Vlan 10 is successfully cleared from vlan group eng-dept.
Console> (enable)

```

This example shows that when all the VLANs are cleared from a VLAN group, the VLAN group is cleared:

```

Console> (enable) clear dot1x vlan-group eng-dept 30
Vlan 30 is successfully cleared from vlan group eng-dept.
Warning: No more vlans mapped to this group, vlan group is cleared.
Console> (enable) show dot1x vlan-group eng-dept
Vlan group eng-dept doesn't exist, can not display.
Console> (enable)

```

This example shows how to clear all the existing VLAN groups:

```
Console> (enable) clear dot1x vlan-group all
Console> (enable) show dot1x vlan-group all
No vlan groups are present for display.
Console> (enable)
```

## Enabling and Disabling 802.1X RADIUS Accounting and Tracking

You can use 802.1X RADIUS accounting and tracking to send the 802.1X user accounting information to the RADIUS server. The feature uses UDP port number 1813.

An 802.1X accounting packet can indicate the following information to the RADIUS server:

- When a user successfully authenticates
- When a user logs off
- When the link goes down on an 802.1X port
- When a reauthentication succeeds
- When a reauthentication fails

The attributes of the accounting packets are as follows (some attributes are optional):

- Attribute [1] USERNAME—The username that is going to be authenticated.
- Attribute [4] NAS-IP—The IP address of the switch that initiated the authentication/accounting session (typically, this is the sc0 interface IP address).
- Attribute [40] ACCT-STATUS-TYPE—START/STOP/INTERIM
  - START is sent when the authentication succeeds and the port is moved to the authorized state.
  - STOP is sent when the user sends a logoff, when the link goes down, or when reauthentication fails.
  - INTERIM is sent when a reauthentication succeeds.
- Attribute [44] ACCT-SESSION-ID—The unique session identifier that is associated with every accounting session.

The accounting packet format is as follows:

```
<NAS-IP> <user-id> <date> <time> <random16bit#>
```

An example of the accounting packet format is as follows:

```
9.9.150.140 rameshp 31/07/2003 12:40:00 12345
```

The attributes listed above are common regardless of the ACCT-STATUS-TYPE attribute (for START/STOP/INTERIM).

These attributes are specific to the INTERIM updates:

- Attribute [8] FRAMED-IP-ADDRESS—The IP address that is assigned to the user (this address can be obtained through a static assignment or through DHCP).

- Attribute [81] TUNNEL-PRIVATE-GROUP-ID—Actual VLAN name that is sent by the RADIUS server.

CISCO-AV-PAIRS sent along with the above attribute in “Interim Accounting Request” are as follows:

- AAA: ip-addr-method—Sent whether the IP assignment is through DHCP or statically configured.
- AAA: vlan-assign-method—Device local or RADIUS assigned.

The type is “device local” when the RADIUS server does not send a VLAN. In that case, the administratively-configured port VLAN is the VLAN for the user. If the RADIUS server sent the VLAN, the type is “RADIUS assigned.”

These attributes are specific to the STOP packets:

- Attribute [49] ACCT-TERMINATION-CAUSE—The cause can be due to a user logoff, a port going down, reauthentication failures, and so on.
- CISCO-AV-PAIRS
  - Cisco:Input-Octets—A 64-byte integer that provides the number of bytes of ingress traffic that is received on the port.
  - Cisco:Output-Octets—A 64-byte integer that provides the number of bytes of egress traffic that is forwarded from the port.

## Using the CLI to Enable and Disable 802.1X RADIUS Accounting and Tracking

To enable or disable 802.1X RADIUS accounting and tracking globally, perform this task in privileged mode (the default is disabled):

Task	Command
Enable or disable 802.1X RADIUS accounting and tracking globally.	<b>set dot1x radius-accounting { enable   disable }</b>

This example shows how to enable or disable 802.1X RADIUS accounting and tracking globally:

```
Console> (enable) set dot1x radius-accounting enable
dot1x radius-accounting enabled.
Console> (enable) set dot1x radius-accounting disable
dot1x radius-accounting disabled.
Console> (enable)
```

## Enabling and Disabling RADIUS Keepalive

Use the **set radius-keepalive enable** command to check if configured RADIUS servers are alive. When the command is enabled, the switch sends out a test username for authentication. In reply to the test username, the RADIUS servers send an access rejection. To turn off authentication attempts that test the RADIUS servers, enter the **set radius-keepalive disable** command. If you disable this feature, the switch does not check the status of the servers, and the RADIUS server logs do not record the test attempts.



### Note

In software releases 7.5 through 8.2, the command that you used to enable or disable the RADIUS keepalive feature was the **set feature dot1x-radius-keepalive** command. In software release 8.3 through 8.5, the command that you used to enable or disable the RADIUS keepalive feature was the **set dot1x radius-keepalive** command. In software release 8.6 and later releases, the command to enable or disable the RADIUS keepalive feature is the **set radius keepalive** command.

To enable or disable the RADIUS keepalive feature, perform this task in privileged mode (the default is enabled):

Task	Command
Enable or disable the RADIUS keepalive feature.	<b>set radius keepalive {enable   disable}</b>

This example shows how to globally enable the RADIUS keepalive feature:

```
Console> (enable) set radius keepalive enable
Radius Keepalive enabled.
Console> (enable)
```

To set the RADIUS keepalive time in seconds, perform this task in privileged mode (the default is 60 seconds):

Task	Command
Set the RADIUS keepalive time. The time can be set from 1–6,000 seconds. The default is 60 seconds.	<b>set radius keepalive time <i>seconds</i></b>

This example shows how to set the RADIUS keepalive time:

```
Console> (enable) set radius keepalive time 120
Radius keepalive time set to 120 seconds.
Console> (enable)
```

## Configuring the Authenticated Identity-to-Port Description Mappings

You can use authenticated identity-to-port description mapping to assign a port name to the 802.1X port based on the information that is received from the RADIUS server. This feature uses an AV-pair “Supplicant Name” to uniquely assign a port name for an authenticated user. Currently, there is support only for the Cisco-supported AV-pairs that are sent from the authentication server; the other vendor-specific AV-pairs are ignored.

Enter the **show port dot1x name-mapping** command to display the name of the port that is received from the RADIUS server. If the switch receives an authenticated port name that is greater than or equal to 20 characters, the name is truncated to 19 characters and a # sign is appended to the name (allowing a total of 20 characters that is compatible with the **set port name** command). When you enter the **set port name** command, the end result is the same as if you had used the authenticated identity-to-port description mapping; the difference is that this feature assigns the name dynamically upon 802.1X authentication. An example of a dynamically assigned port name is as follows:

```
Console> (enable) show port dot1x name-mapping 5/1
Port Port Name                               802.1X Port Name
-----
5/1  Cube-C1/2                                User1
```

## Configuring the DNS Resolution for a RADIUS Server Configuration

When you configure the DNS resolution for a RADIUS server, you can configure the RADIUS server using a DNS name in addition to the IP addresses. The switch automatically resolves the DNS name using a DNS server that is configured to associate a DNS name with an IP address. The configured DNS name can coexist with the other IP addresses that are configured as primary or secondary. The DNS name is stored in NVRAM. You must enable the RADIUS keepalive feature for the DNS resolution to work. DNS resolution allows you to modify the IP address of the RADIUS server transparently without the knowledge of the switch. The switch can then resolve the DNS name with the modified IP address.

The switch resolves the DNS name a second time (reresolution) to the IP address during the initial configuration of the DNS name, when 802.1X is disabled and enabled, during the 802.1X port authentication, or if the request to the RADIUS server times out. The reresolution checks if the DNS name-to-IP address mapping is changed on the DNS server side.

Enter the **show config** or **show radius** commands to display the DNS name if the DNS name is configured in place of an IP address for the RADIUS server. You can configure a maximum of three RADIUS servers. To display the configured RADIUS server parameters, enter the **show radius** command as follows:

```
Console> (enable) show radius
RADIUS Deadtime:          0 minutes
RADIUS Key:               cisco
RADIUS Retransmit:       2
RADIUS Timeout:          5 seconds
Framed-IP Address Transmit: Disabled

RADIUS-Server              Status  Auth-port  Acct-port  Resolved IP Address
-----
9.9.150.16                 primary 1812       1813
cat6k-sup2                 1812    1813       9.9.150.20
cat6k-sup3                 1812    1813       9.9.150.21
Console> (enable)
```

## Configuring the Authentication Failure VLAN

On a traditional 802.1X port, the switch does not provide access to the network until the supplicant that is connected to the port is authenticated by verifying its identity information with an authentication server. With the authentication failure VLAN feature, you can configure the authentication failure VLAN on a per-port basis and that after three failed 802.1X authentication attempts by the supplicant, the port is moved to the authentication failure VLAN where the supplicant can access the network.



### Note

Contrast an authentication failure VLAN with a guest VLAN. A guest VLAN enables the non-802.1X capable hosts to access the networks that use 802.1X authentication. You can use the guest VLANs while you are upgrading your system to support the 802.1X authentication. Typically, the guest VLANs support minimal services and provide minimal network access.

An authentication failure VLAN is independent of a guest VLAN. However, the guest VLAN can be the same VLAN as the authentication failure VLAN. If you do not want to differentiate between the non-802.1X capable hosts and the authentication failed hosts, you may configure both hosts to the same VLAN (either a guest VLAN or an authentication failure VLAN).

For more information, see the [“Understanding How 802.1X Authentication for the Guest VLAN Works” section on page 40-9.](#)

## Authentication Failure VLAN Configuration Guidelines and Restrictions

This section describes the configuration guidelines and restrictions for configuring the authentication failure VLAN:

- After three failed 802.1X authentication attempts by the supplicant, the port is moved to the authentication failure VLAN where the supplicant can access the network. These three attempts introduce a delay of 3 minutes before the port is enabled in the authentication failure VLAN and the EAP success packet is sent to the supplicant (1 minute per failed attempt based on the default quiet period of 60 seconds after each failed attempt).
- The number of failed 802.1X authentication attempts is counted from the time of the linkup to the point where the port is moved into the authentication failure VLAN. When the port moves into the authentication failure VLAN, the failed-attempts counter is reset.
- Only the authenticated failed users are moved to the authentication failure VLAN.
- The authentication failure VLAN is supported only in the single-authentication mode (the default port mode).
- The authentication failure VLAN is not supported on a port that is configured as a unidirectional port.
- The supplicant’s MAC address is added to the CAM table and only its MAC address is allowed on the authentication failure VLAN port. Any new MAC address appearing on the port is treated as a security violation.
- The authentication failure VLAN port cannot be part of an RSPAN VLAN or a private VLAN.



### Note

In software release 8.6(1) and later releases, a private VLAN and secondary VLAN can be configured as the guest VLAN or authentication failure VLAN. For more information, see the [“Configuring 802.1X Authentication with Private VLANs” section on page 40-41.](#)

- On multiple VLAN access ports (MVAPs), the authentication failure VLAN and the auxiliary VLAN cannot be the same VLAN.
- The authentication failure VLAN and port security features do not conflict with each other. Additionally, other security features, such as Dynamic ARP Inspection (DAI), Dynamic Host Configuration Protocol (DHCP) snooping, and IP source guard can be enabled and disabled independently on the authentication failure VLAN.
- An authentication failure VLAN is independent of a guest VLAN. However, the guest VLAN can be the same VLAN as the authentication failure VLAN. If you do not want to differentiate between the non-802.1X capable hosts and the authentication failed hosts, you may configure both hosts to the same VLAN (either a guest VLAN or an authentication failure VLAN).
- High availability is supported with an authentication failure VLAN.

## Creating an Authentication Failure VLAN and Adding 802.1X Ports

To create an authentication failure VLAN and add 802.1X ports to the VLAN, perform this task in privileged mode:

Task	Command
Create an authentication failure VLAN and add 802.1X ports to the VLAN.	<b>set port dot1x mod/ports auth-fail-vlan { none   vlan }</b>

This example shows how to create the authentication failure VLAN (VLAN 81) and add port 3/33:

```
Console> (enable) set port dot1x 3/33 auth-fail-vlan 81
Port 3/33 Auth Fail Vlan is set to 81
Console> (enable)
```

This example shows how to display the authentication failure VLAN configuration:

```
Console> (enable) show port dot1x auth-fail-vlan
Auth-Fail-Vlan Status Mod/Ports
-----
81 active 3/33
none none 1/1-2,2/1-2,3/1-32,3/34-48
Console> (enable)
```

This example shows how to clear a port from an authentication failure VLAN:

```
Console> (enable) set port dot1x 3/33 auth-fail-vlan none
Port 3/33 Auth Fail Vlan is cleared
Console> (enable)
```

This example shows how to list the active users and ports in an authentication failure VLAN:

```
Console> (enable) show dot1x auth-fail-users
Username Mod/Port Auth-Fail-Vlan
-----
testuser 3/33 81
Console> (enable)
```

## Configuring a RADIUS Server Failover

Before software release 8.4(1), when the active RADIUS server went down or was unreachable, the 802.1X authentication timed out before the backup RADIUS server could become active. With software release 8.4(1) and later releases, some RADIUS server timer values are now configurable and the **show radius** command has been enhanced to show the active RADIUS server.

Enter the following commands to prevent a RADIUS server failover:

- **set dot1x max-req**—Specifies the maximum number of times that the state machine retransmits an EAP-Request frame to the supplicant before it times out the authentication session; the valid values are from 1 to 10. The default is 2. An example is as follows:

```
Console> (enable) set dot1x max-req 8
dot1x max-req set to 8.
Console> (enable)
```

- **set dot1x server-timeout**—Specifies the time constant for the retransmission of packets by the back-end authenticator to the authentication server; the valid values are from 1 to 65535 seconds. When the authentication server does not notify the back-end authenticator that it received specific packets, the back-end authenticator waits a period of time (set by entering the **server-timeout seconds** parameter), and then retransmits the packets. The default is 30. An example is as follows:

```
Console> (enable) set dot1x server-timeout 100
dot1x server-timeout set to 100 seconds.
Console> (enable)
```

Enter the **show radius** command to display the RADIUS server configuration and to show which RADIUS server is active as follows:

```
Console> (enable) show radius
Active RADIUS Server:      81.81.81.20
RADIUS Deadtime:          1 minutes
RADIUS Key:                cisco
RADIUS Retransmit:         2
RADIUS Timeout:           5 seconds
Framed-IP Address Transmit: Disabled

RADIUS-Server              Status  Auth-port  Acct-port  Resolved IP Address
-----
81.81.81.20                 primary 1812       1813
10.6.89.200                 1812    1813
10.6.98.35                  1812    1813
Console> (enable)
```

# Configuring 802.1X Authentication with Private VLANs

**Note**

For more information on private VLANs, see the [“Configuring Private VLANs on the Switch”](#) section on page 11-19.

These sections describe how to configure 802.1X authentication with private VLANs:

- [Overview, page 40-41](#)
- [Port VLANs and 802.1X VLANs, page 40-41](#)
- [Configuration Guidelines, page 40-42](#)
- [Configuring 802.1X Authentication with Private VLANs, page 40-42](#)

## Overview

Private VLANs provide a subnet conservation mechanism that allows a port to be conditionally operational in a VLAN pair without trunking. A private VLAN is composed of an associated primary VLAN and a secondary VLAN. A primary VLAN can participate in multiple private VLANs, with each primary VLAN having a different secondary VLAN associated with it. A secondary VLAN must belong to only one private VLAN. The secondary VLAN must be associated with only one primary VLAN. Secondary VLAN types are community, isolated, and two-way.

Before software release 8.6(1), an 802.1X port could not be configured in a private VLAN and a private VLAN port could not participate in 802.1X. With software release 8.6(1) and later releases, you can enable isolated private VLANs for 802.1X ports that are assigned to a guest VLAN through 802.1X authentication.

With guest VLANs, you might have ports from different customers residing in the same guest VLAN if the supplicant is identified as incapable of 802.1X before becoming 802.1X capable. With this behavior, the traffic from one customer might be accessible to every other customer. To avoid this situation, you can select different guest VLANs for each port; however, this action consumes multiple VLANs. With the isolated private VLAN approach, you can configure multiple ports in a VLAN pair and suppress the traffic interchange between the ports in the same secondary VLAN.

## Port VLANs and 802.1X VLANs

With 802.1X, a port can be in a preauthenticated or post-authenticated state. In both states, the port is associated with a VLAN. The VLANs are referred to as the port VLAN and the 802.1X VLAN. The port VLAN is the VLAN of the port before a new VLAN has been assigned by 802.1X. The 802.1X VLAN of the port is the VLAN that is assigned to the port by 802.1X. The port operates in its port VLAN if it has not been enabled for 802.1X. Once the port is enabled for 802.1X, the port continues to be associated with its port VLAN although it stops forwarding traffic on the port VLAN. Once 802.1X assigns a new VLAN to the port, the port becomes operationally associated with the new VLAN (the 802.1X VLAN). If no VLAN is supplied by the RADIUS server, the port becomes operational in its port VLAN. A summary of port VLAN and 802.1X VLAN behavior follows:

- The port VLAN behavior is as follows:
  - Used by ports before 802.1X is enabled
  - Used as a nonoperational port VLAN after 802.1X is enabled

- Used as a nonoperational port VLAN before the port reaches an 802.1X state (authenticated, guest VLAN, or authentication failure VLAN)
- Used as an operational VLAN in the authenticated state if no VLAN is provided by the RADIUS server
- Can be a private VLAN
- The 802.1X VLAN behavior is as follows:
  - Used as an operational port VLAN after 802.1X moves the port to an 802.1X state (authenticated, guest VLAN, or authentication failure VLAN)
  - Can be a private VLAN

## Configuration Guidelines

This section provides the guidelines for configuring 802.1X authentication with private VLANs:

- No changes to the existing CLI are required for configuring 802.1X authentication with private VLANs.
- When you add an 802.1X port to a VLAN (RADIUS-assigned VLAN, guest VLAN, or authentication failure VLAN), the following checks are automatically made:
  - It is verified that the private VLAN is a secondary VLAN
  - It is verified that the secondary VLAN is associated to a valid primary VLAN

If any of the checks fail, an error message is generated and the port is not placed in the private VLAN.

- Promiscuous ports and the sc0 interface cannot participate in 802.1X.
- When you configure an 802.1X port in a private VLAN, BPDU guard is automatically enabled, trunking is set to off, and the port retains these settings after being removed from the private VLAN.
- IP phone ports that support 802.1X cannot be private VLAN ports.

## Configuring 802.1X Authentication with Private VLANs

These sections describe and provide examples on configuring 802.1X authentication with private VLANs:

- [Creating Private VLANs, page 40-43](#)
- [Verifying the Private VLAN Configuration, page 40-43](#)
- [Verifying the Pre-802.1X Port Settings, page 40-44](#)
- [Assigning Private VLANs to 802.1X, page 40-45](#)
- [Verifying the Config-Time 802.1X Private VLAN Settings, page 40-45](#)
- [Verifying the Run-Time 802.1X-Assigned Private VLAN Settings, page 40-45](#)

## Creating Private VLANs

This example shows how to create private VLANs:

```
Console> (enable) set vlan 800 pvlan-type primary
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 800 configuration successful
Console> (enable) set vlan 801 pvlan-type community
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 801 configuration successful
Console> (enable) set pvlan 800 801
Host mode set to enable for ports
BPDU guard set to enable for ports
Trunk mode set to off for ports
Successfully set association between 800 and 801.
Console> (enable) set vlan 400 pvlan-type primary
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 400 configuration successful
Console> (enable) set vlan 401 pvlan-type isolated
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 401 configuration successful
Console> (enable) set pvlan 400 401
Host mode set to enable for ports
BPDU guard set to enable for ports
Trunk mode set to off for ports
Successfully set association between 400 and 401.
Console> (enable) set vlan 200 pvlan-type primary
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 200 configuration successful
Console> (enable) set vlan 201 pvlan-type twoway-community
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 201 configuration successful
Console> (enable) set pvlan 200 201
Host mode set to enable for ports
BPDU guard set to enable for ports
Trunk mode set to off for ports
Successfully set association between 200 and 201.
Console> (enable)
```

## Verifying the Private VLAN Configuration

This example shows how to verify the private VLAN configuration:

```
Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports
-----
200 201 twoway-community
400 401 isolated
800 801 community
Console> (enable)
```

## Verifying the Pre-802.1X Port Settings

This example shows how to verify the pre-802.1X port settings:

```

Console> (enable) show port 2/2
* = Configured MAC Address
# = 802.1X Authenticated Port Name.
Port Name Status Vlan Duplex Speed Type
-----
2/2 connected 999 a-half a-10 10/100BaseTX
Port AuxiliaryVlan AuxVlan-Status
-----
2/2 none none
Port Security Violation Shutdown-Time Age-Time Max-Addr Trap IfIndex
-----
2/2 disabled shutdown 0 0 1 disabled 61
Port Flooding on Address Limit Last-Src-Addr Vlan TimerType
-----
2/2 Enabled - - Absolute
Port Num-Addr Secure-Src-Addr Vlan Age-Left Shutdown/Time-Left
-----
2/2 0 - - - -
Port 802.1X Auth-State 802.1X Port-Status
-----
2/2 force-authorized authorized
Port Broadcast-Limit Multicast Unicast Total-Drop Action
-----
2/2 - - - 0 drop-packets
Port Send FlowControl Receive FlowControl RxPause TxPause
admin oper admin oper
-----
2/2 off off off off 0 0
Port Status Channel Admin Ch
Mode Group Id
-----
2/2 connected off 2 0
Port Status ErrDisable Reason Port ErrDisableTimeout Action on Timeout
-----
2/2 connected - Enable No Change
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
-----
2/2 0 0 0 0 0
Port Single-Col Multi-Coll Late-Coll Excess-Col Carri-Sen Runts Giants
-----
2/2 3 3 0 3 0 0 0
Port Last-Time-Cleared
-----
2/2 Mon Oct 3 2005, 12:42:26
Idle Detection
-----
Console> (enable) show port dot1x 2/2
Port Auth-State BEnd-State Port-Control Port-Status
-----
2/2 force-authorized idle force-authorized authorized
Port Port-Mode Re-authentication Shutdown-timeout Control-Mode
admin oper
-----
2/2 SingleAuth disabled disabled Both Both
Port Posture-Token Critical Termination action Session-timeout
-----
2/2 - NO NoReAuth -
Console> (enable)

```

## Assigning Private VLANs to 802.1X

This example shows how to assign private VLANs to 802.1X:

```

Console> (enable) set port dot1x 2/2 port-control auto
Port 2/2 dot1x port-control is set to auto.
Trunking disabled for port 2/2 due to Dot1x feature.
Spanntree port fast start option enabled for port 2/2.
Console> (enable) set port dot1x 2/2 initialize
Port 2/2 dot1x initializing ...
Console> (enable) set port dot1x 2/2 port-control auto
Port 2/2 dot1x port-control is set to auto.
Trunking disabled for port 2/2 due to Dot1x feature.
Spanntree port fast start option enabled for port 2/2.
Console> (enable) set port dot1x 2/2 initialize
Port 2/2 dot1x initializing ...
Console> (enable) set port dot1x 2/2 guest-vlan 401
Port 2/2 Guest Vlan is set to 401
Console> (enable) set port dot1x 2/2 auth-fail-vlan 201
Port 2/2 Auth Fail Vlan is set to 201
Console> (enable)

```

## Verifying the Config-Time 802.1X Private VLAN Settings

This example shows how to verify the config-time 802.1x private VLAN settings:

```

Console> (enable) show port 2/2
* = Configured MAC Address
# = 802.1X Authenticated Port Name.
Port Name Status Vlan Duplex Speed Type
-----
2/2 connected 999 a-half a-10 10/100BaseTX
<...snip...>
Console> (enable) show port dot1x 2/2
Port Auth-State BEnd-State Port-Control Port-Status
-----
2/2 connecting idle auto unauthorized
<...snip...>
Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports
-----
200 201 twoway-community
400 401 isolated
800 801 community
Console> (enable)

```

## Verifying the Run-Time 802.1X-Assigned Private VLAN Settings

This example shows how to verify the run-time 802.1X-assigned private VLAN settings:

```

Console> (enable) show port dot1x guest-vlan
Guest-Vlan Status Mod/Ports
-----
401 active 2/2
none none 2/1,2/3-48,3/1-48,5/1-2
Console> (enable) show port dot1x auth-fail-vlan
Auth-Fail-Vlan Status Mod/Ports
-----
201 active 2/2
none none 2/1,2/3-48,3/1-48,5/1-2
Console> (enable)

```

**Example 1: Guest VLAN is an isolated private VLAN (VLANs 400, 401)**

```

Console> (enable) show port 2/2
* = Configured MAC Address
# = 802.1X Authenticated Port Name.
Port Name Status Vlan Duplex Speed Type
-----
2/2 connected guest-400,401 a-half a-10 10/100BaseTX
<...snip...>
Console> (enable) show port dot1x 2/2
Port Auth-State BEnd-State Port-Control Port-Status
-----
2/2 guest-vlan idle auto authorized
<...snip...>
Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports
-----
200 201 twoway-community
400 401 isolated 2/2
800 801 community
Console> (enable)

```

**Example 2: 802.1X authentication failure VLAN is a two-way community private VLAN (VLANs 200, 201)**

```

Console> (enable) show port 2/2
* = Configured MAC Address
# = 802.1X Authenticated Port Name.
Port Name Status Vlan Duplex Speed Type
-----
2/2 connected fail-200,201 a-half a-10 10/100BaseTX
<...snip...>
Console> (enable) clear port dot1x 2/2
dot1x port statistics cleared successfully for port
Console> (enable) show port dot1x 2/2
Port Auth-State BEnd-State Port-Control Port-Status
-----
2/2 auth-fail idle auto authorized
<...snip...>
Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports
-----
200 201 twoway-community 2/2
400 401 isolated
800 801 community
Console> (enable)

```

**Example 3: 802.1X RADIUS-supplied VLAN is a community private VLAN (VLANs 800, 801)**

```

Console> (enable) show port 2/2
* = Configured MAC Address
# = 802.1X Authenticated Port Name.
Port Name Status Vlan Duplex Speed Type
-----
2/2 connected dot1x-800,801 a-half a-10 10/100BaseTX
Port AuxiliaryVlan AuxVlan-Status
-----
2/2 none none
Port Security Violation Shutdown-Time Age-Time Max-Addr Trap IfIndex
-----
2/2 disabled shutdown 0 0 1 disabled 61
Port Flooding on Address Limit Last-Src-Addr Vlan TimerType
-----

```

```

2/2 Enabled - - Absolute
Port Num-Addr Secure-Src-Addr Vlan Age-Left Shutdown/Time-Left
-----
2/2 0 - - - -
<...snip...>
Console> (enable) show port dot1x 2/2
Port Auth-State BEnd-State Port-Control Port-Status
-----
2/2 authenticated idle auto authorized
<...snip...>
Console> (enable) show pvlan
Primary Secondary Secondary-Type Ports
-----
200 201 twoway-community
400 401 isolated
800 801 community 2/2
Console> (enable)

```

## Using the show Commands

Use these **show** commands to access the information about 802.1X authentication and its configuration:

- **show port dot1x ?**
- **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 <b>show port dot1x</b> command.	<b>show port dot1x ?</b>

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

```

Console> (enable) show port dot1x ?
  guest-vlan          Show Port guest vlan information
  statistics          Show statistic information
  <mod>               Module number
  <mod/port>          Module number and Port number(s)
  |                   Output modifiers
  <cr>

```

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 the configurable and current state parameters that are associated with the authenticator PAE and back-end authenticator on a specific port on a specific module.	<b>show port dot1x mod/port</b>

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 3:

```

Console> (enable) show port dot1x 3/1
Port  Auth-State      BEnd-State  Port-Control  Port-Status
-----
 3/1  connecting        idle        auto          unauthorized

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
 3/1  SingleAuth    enabled           disabled          In      oper
-----
Console> (enable)

```

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.	<b>show port dot1x statistics mod/port</b>

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 3:

```

Console> (enable) show port dot1x statistics 3/1
Port  Tx_Req/Id Tx_Req Tx_Total Rx_Start Rx_Logoff Rx_Resp/Id Rx_Resp
-----
 3/1  43        0     43        0        0        0        0

Port  Rx_Invalid Rx_Len_Err Rx_Total Last_Rx_Frm_Ver Last_Rx_Frm_Src_Mac
-----
 3/1  2          0         2         0          00-00-00-00-00-00
-----
Console> (enable)

```

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.	<b>show dot1x</b>

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
radius-accounting       disabled
radius-vlan-assignment enabled
radius-keepalive state  enabled
re-authperiod           7200 seconds
server-timeout          30 seconds
shutdown-timeout        300 seconds

```

```

supp-timeout          30 seconds
tx-period             30 seconds

```

```
Console> (enable)
```

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

Task	Command
Display the 802.1X authenticated MAC addresses.	<b>show cam static</b>

This example shows how to display the 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)

```

