

Configuring 802.1X Port-Based Authentication

This chapter describes how to configure IEEE 802.1X port-based authentication to prevent unauthorized client devices from gaining access to the network.

This chapter includes the following major sections:

- [Understanding 802.1X Port-Based Authentication, page 37-1](#)
- [Configuring 802.1X, page 37-21](#)
- [Displaying 802.1X Statistics and Status, page 37-48](#)

**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm>

Understanding 802.1X Port-Based Authentication

802.1X defines 802.1X port-based authentication as a client-server based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. An authentication server validates each supplicant (client) connected to an authenticator (network access switch) port before making available any services offered by the switch or the LAN.

**Note**

802.1X support requires an authentication server that is configured for Remote Authentication Dial-In User Service (RADIUS). 802.1X authentication does not work unless the network access switch can route packets to the configured RADIUS server. To verify that the switch can route packets, you must ping the server from the switch.

Until a client is authenticated, only Extensible Authentication Protocol over LAN (EAPOL) traffic is allowed through the port to which the client is connected. After authentication succeeds, normal traffic can pass through the port.

To configure 802.1X port-based authentication, you need to understand the concepts in these sections:

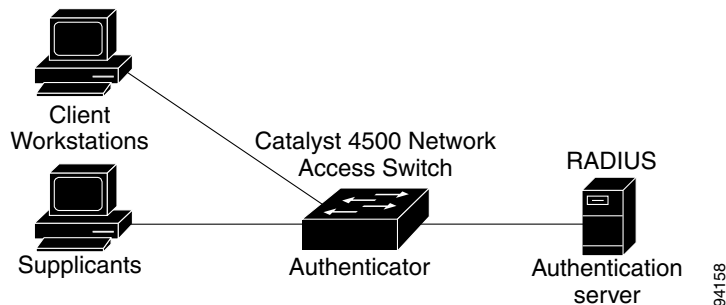
- [Device Roles, page 37-2](#)
- [802.1X and Network Access Control, page 37-3](#)
- [Authentication Initiation and Message Exchange, page 37-3](#)

- Ports in Authorized and Unauthorized States, page 37-4
- 802.1X Host Mode, page 37-6
- Using 802.1X with VLAN Assignment, page 37-7
- Using 802.1X for Guest VLANs, page 37-8
- Using 802.1X with MAC Authentication Bypass, page 37-9
- Using 802.1X with Inaccessible Authentication Bypass, page 37-12
- Using 802.1X with Unidirectional Controlled Port, page 37-12
- Using 802.1X with Authentication Failed VLAN Assignment, page 37-13
- Using 802.1X with Port Security, page 37-15
- Using 802.1X with RADIUS-Provided Session Timeouts, page 37-16
- Using 802.1X with RADIUS Accounting, page 37-16
- Using 802.1X with Voice VLAN Ports, page 37-19
- Using Multiple Domain Authentication, page 37-19
- Supported Topologies, page 37-21

Device Roles

With 802.1X port-based authentication, network devices have specific roles. Figure 37-1 shows the role of each device, which is described below.

Figure 37-1 802.1X Device Roles



- Client—The workstation that requests access to the LAN, and responds to requests from the switch. The workstation must be running 802.1X-compliant client software.



Note For more information on 802.1X-compliant client application software such as Microsoft Windows 2000 Professional or Windows XP, refer to the Microsoft Knowledge Base article at this URL: <http://support.microsoft.com>

- Authenticator—Controls physical access to the network based on the authentication status of the client. The Catalyst 4500 series switch acts as an intermediary between the client and the authentication server, requesting identity information from the client, verifying that information

with the authentication server, and relaying a response to the client. The switch encapsulates and decapsulates the Extensible Authentication Protocol (EAP) frames and interacts with the RADIUS authentication server.

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



Note The Catalyst 4500 series switches must be running software that supports the RADIUS client and 802.1X.

- Authentication server—Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch that the client is authorized to access the LAN and switch services. (The only supported authentication server is the RADIUS authentication server with EAP extensions; it is available in Cisco Secure Access Control Server version 3.2 and later.)

802.1X and Network Access Control

Network Access Control is a feature that allows port access policies to be influenced by the anti-virus posture of the authenticating device.

Anti-virus posture includes such elements as the operating system running on the device, the operating system version, whether anti-virus software is installed, what version of anti-virus signatures is available, etc. If the authenticating device has a NAC-aware 802.1X supplicant and the authentication server is configured to support NAC via 802.1X, anti-virus posture information is automatically included as part of the 802.1X authentication exchange.

For information on configuring NAC, refer to the URL:

http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_configuration_guide09186a00805764fd.html

Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port with the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state has changed. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

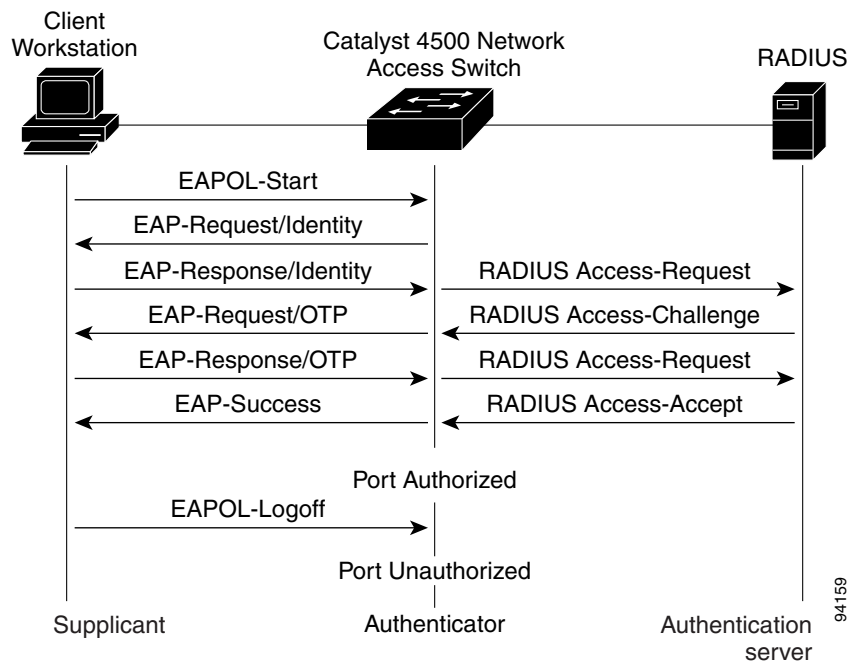
However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

If 802.1X is not enabled or supported on the network access switch, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state means that the client has been successfully authenticated. When the client supplies its identity, the

switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. [Figure 37-2](#) shows a message exchange that is initiated by the client using the One-Time Password (OTP) authentication method with an authentication server.

Figure 37-2 Message Exchange



Ports in Authorized and Unauthorized States

The switch port state determines whether or not the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a non-802.1X capable client is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network. If a guest VLAN is configured on a port that connects to a client that does not support 802.1X, the port is placed in the configured guest VLAN and in the authorized state. For more information, see the [“Using 802.1X for Guest VLANs” section on page 37-8](#).

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

You can control the port authorization state with the **dot1x port-control** interface configuration command and these keywords:

- **force-authorized**—Disables 802.1X authentication and causes the port to transition to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This setting is the default.
- **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.
- **auto**—Enables 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch can uniquely identify each client attempting to access the network by the client's MAC address.

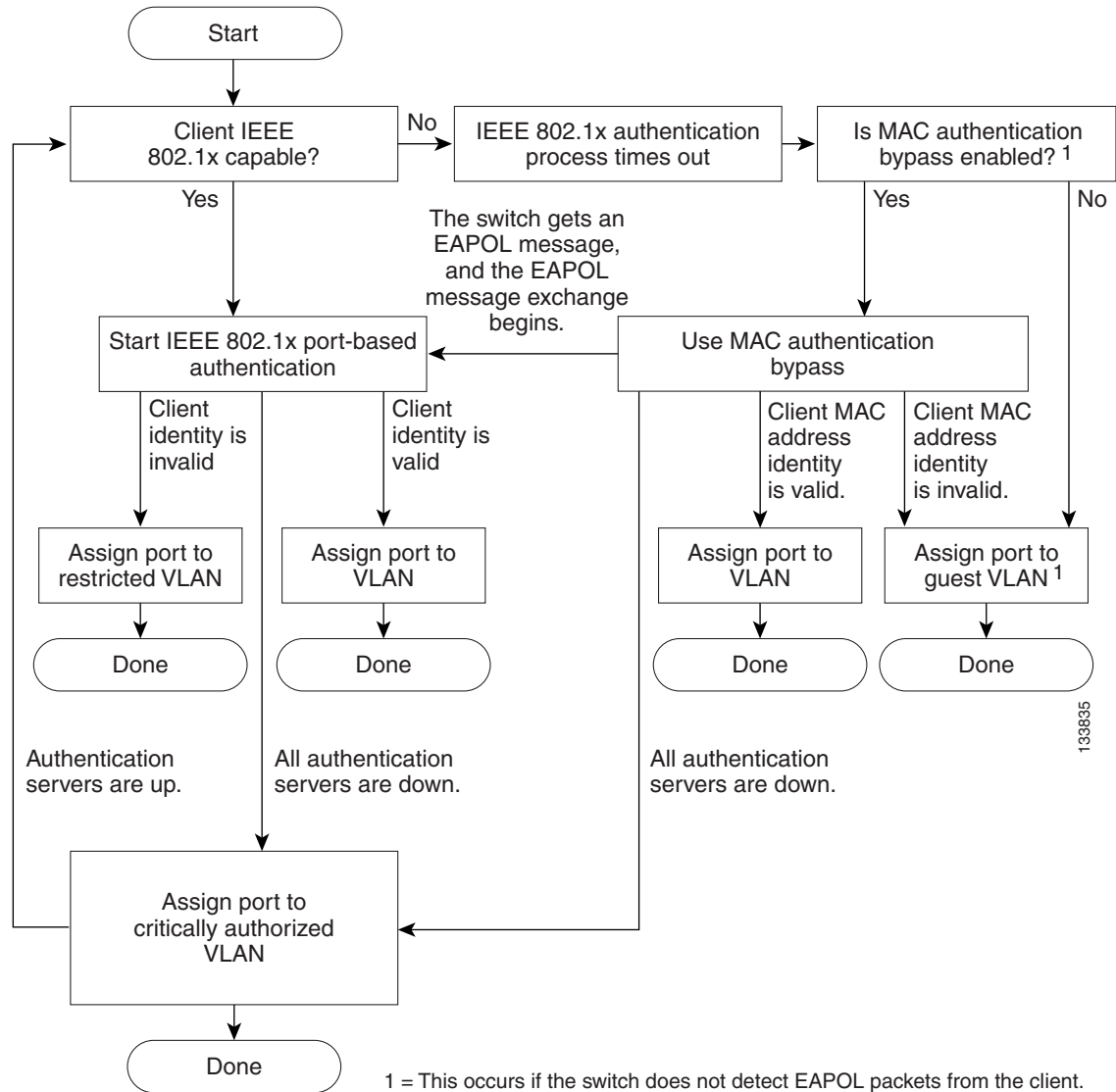
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch 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.

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

[Figure 37-3](#) shows the authentication process.

If Multidomain Authentication (MDA) is enabled on a port, this flow can be used with some exceptions that are applicable to voice authorization. For more information on MDA, see [“Using Multiple Domain Authentication”](#) section on page 37-19.

Figure 37-3 Authentication Flowchart



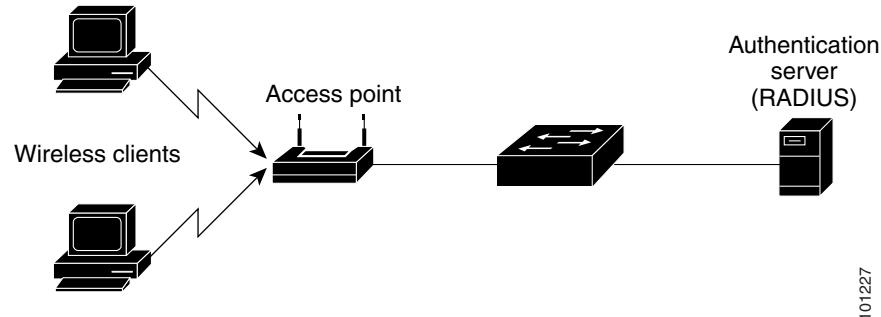
802.1X Host Mode

You can configure an 802.1X port for single-host or multiple-hosts mode. In single-host mode (see [Figure 37-1 on page 37-2](#)), only one client can be connected to the 802.1X-enabled switch port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

In multiple-hosts mode, you can attach multiple hosts to a single 802.1X-enabled port. [Figure 37-4 on page 37-7](#) shows 802.1X port-based authentication in a wireless LAN. In this mode, only one of the attached clients must be authorized for all clients to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logout message is received), the switch denies network access to all of the attached clients. In this topology, the wireless access point is responsible for authenticating the clients attached to it, and it also acts as a client to the switch.

With multiple-hosts mode enabled, you can use 802.1X authentication to authenticate the port and port security to manage network access for all MAC addresses, including that of the client.

Figure 37-4 Multiple Host Mode Example



Cisco IOS Release 12.2(37)SG and later releases support Multi-Domain Authentication (MDA), which allows both a data device and a voice device, such as an IP Phone (Cisco or non-Cisco), to connect to the same switch port. For details on how to configure MDA, see the [“Using Multiple Domain Authentication”](#) section on page 37-19.

Using 802.1X with VLAN Assignment

You can use the VLAN assignment to limit network access for certain users. With the VLAN assignment, 802.1X-authenticated ports are assigned to a VLAN based on the username of the client connected to that port. The RADIUS server database maintains the username-to-VLAN mappings. After successful 802.1X authentication of the port, the RADIUS server sends the VLAN assignment to the switch. The VLAN can be a “standard” VLAN or a PVLAN.

On platforms that support PVLANS, you can isolate hosts by assigning ports into PVLANS.

When configured on the switch and the RADIUS server, 802.1X with VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server, the port is configured in its access VLAN or isolated PVLAN when authentication succeeds.
- If the authentication server provides invalid VLAN information, the port remains unauthorized. This situation prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error.
- If the authentication server provides valid VLAN information, the port is authorized and placed in the specified VLAN when authentication succeeds.
- If the multiple-hosts mode is enabled, all hosts are in the same VLAN as the first authenticated user.
- If 802.1X is disabled on the port, the port is returned to the configured access VLAN.
- A port must be configured as an access port (which can be assigned only into “regular” VLANs), or as a PVLAN host port (which can be assigned only into PVLANS). Configuring a port as a PVLAN host port implies that all hosts on the port are assigned into PVLANS, whether their posture is compliant or non-compliant. If the type of the VLAN named in the Access-Accept does not match the type of VLAN expected to be assigned to the port (regular VLAN to access port, secondary private VLAN to private VLAN host port), the VLAN assignment fails.

- If a guest VLAN is configured to handle non-responsive hosts, the type of VLAN configured as the guest VLAN must match the port type (that is, guest VLANs configured on access ports must be standard VLANs, and guest VLANs configured on PVLAN host ports must be PVLANS. If the guest VLAN's type does not match the port type, non-responsive hosts are treated as if no guest VLAN is configured (that is, they are denied network access).
- To assign a port into a PVLAN, the named VLAN must be a secondary PVLAN. The switch determines the implied primary VLAN from the locally configured secondary-primary association.

**Note**

If you change the access VLAN or PVLAN host VLAN mapping on a port that is already authorized in a RADIUS assigned VLAN, the port remains in the RADIUS assigned VLAN.

To configure VLAN assignment you need to perform these tasks:

- Enable AAA authorization with the **network** keyword to allow interface configuration from the RADIUS server. For an illustration of how to apply the **aaa authorization network group radius** command, refer to the section “Enabling 802.1X Authentication” on page 23.
- Enable 802.1X. (The VLAN assignment feature is automatically enabled when you configure 802.1X on an access port.)
- Assign vendor-specific tunnel attributes in the RADIUS server. To ensure proper VLAN assignment, the RADIUS server must return these attributes to the switch:
 - Tunnel-Type = VLAN
 - Tunnel-Medium-Type = 802
 - Tunnel-Private-Group-ID = VLAN NAME

Using 802.1X for Guest VLANs

**Note**

Supervisor Engine 6-E does *not* support this feature.

You can use guest VLANs to enable non-802.1X-capable hosts to access networks that use 802.1X authentication. For example, you can use guest VLANs while you are upgrading your system to support 802.1X authentication.

Guest VLANs are supported on a per-port basis, and you can use any VLAN as a guest VLAN as long as its type matches the type of the port. If a port is already forwarding on the guest VLAN and you enable 802.1X support on the network interface of the host, the port is immediately moved out of the guest VLAN and the authenticator waits for authentication to occur.

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

If the port is configured as a PVLAN host port, the guest VLAN must be a secondary PVLAN. If the port is configured as an access port, the guest VLAN must be a regular VLAN. If the guest VLAN configured on a port is not appropriate for the type of the port, the switch behaves as if no guest VLAN is configured (that is, non-responsive hosts are denied network access).

For details on how to configure guest VLANs, see the [“Configuring 802.1X with Guest VLANs” section on page 37-32](#).

Usage Guidelines for Using 802.1X Authentication with Guest VLANs

The usage guidelines for using 802.1X authentication with guest VLANs are as follows:

- When you reconfigure a guest VLAN to a different VLAN, any authentication failed ports are also moved and the ports stay in their current authorized state.
- When you shut down or remove a guest VLAN from the VLAN database, any authentication failed ports are immediately moved to an unauthorized state and the authentication process is restarted.



Note

No periodic reauthentication is allowed with guest VLANs.

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

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

- If the host fails to respond to the authenticator, the port attempts to connect three times (with a 30 second timeout between each attempt). After this time, the login/password window does not appear on the host, so you must unplug and reconnect the network interface cable.
- Hosts responding with an incorrect login/password fail authentication. Hosts failing 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 authentication the third time, the port is placed in the unauthorized state, and you must disconnect and reconnect the network interface cable.

Using 802.1X with MAC Authentication Bypass

The 802.1X protocol has 3 entities: client (supplicant), authenticator, and authentication server. Typically, the host PC runs the supplicant software and tries to authenticate itself by sending its credentials to the authenticator which in turn relays that info to the authentication server for authentication.

However, not all hosts may have supplicant functionality. Devices that cannot authenticate themselves using 802.1X, which still should have network access, can use MAC Authentication Bypass (MAB), which uses the connecting device's MAC address to grant/deny network access.

Typically, you would use this feature on ports where devices such as printers are connected. Such devices do not have 802.1X supplicant functionality.

In a typical deployment, the RADIUS server maintains a database of MAC addresses that require access. When this feature detects a new MAC address on a port, it generates a RADIUS request with both username and password as the device's MAC address. After authorization succeeds, the port is accessible to the particular device through the same code path that 802.1X authentication would take when processing an 802.1X supplicant. If authentication fails, the port moves to the guest VLAN if configured, or it remains unauthorized.

The Catalyst 4500 series switch also supports re-authentication of MACs on a per port level. Be aware that the re-authentication functionality is provided by 802.1X and is not MAB specific. In the re-authentication mode, a port stays in the previous RADIUS-sent VLAN and tries to re-authenticate itself. If the re-authentication succeeds, the port stays in the RADIUS-sent VLAN. Otherwise, the port becomes unauthorized and moves to the guest VLAN if one is configured.

For details on how to configure MAB, see the [“Configuring 802.1X with MAC Authentication Bypass” section on page 37-35](#).

Feature Interaction

This section lists feature interactions and restrictions when MAB is enabled. If a feature is not listed, assume that it interacts seamlessly with MAB (such as Unidirectional Controlled Port).

- MAB can only be enabled if 802.1X is configured on a port. MAB functions as a fall back mechanism for authorizing MACs. If you configure both MAB and 802.1X on a port, the port attempts to authenticate using 802.1X. If the host fails to respond to EAPOL requests and MAB is configured, the 802.1X port is opened up to listen to packets and to grab a MAC address, rather than attempt to authenticate endlessly.

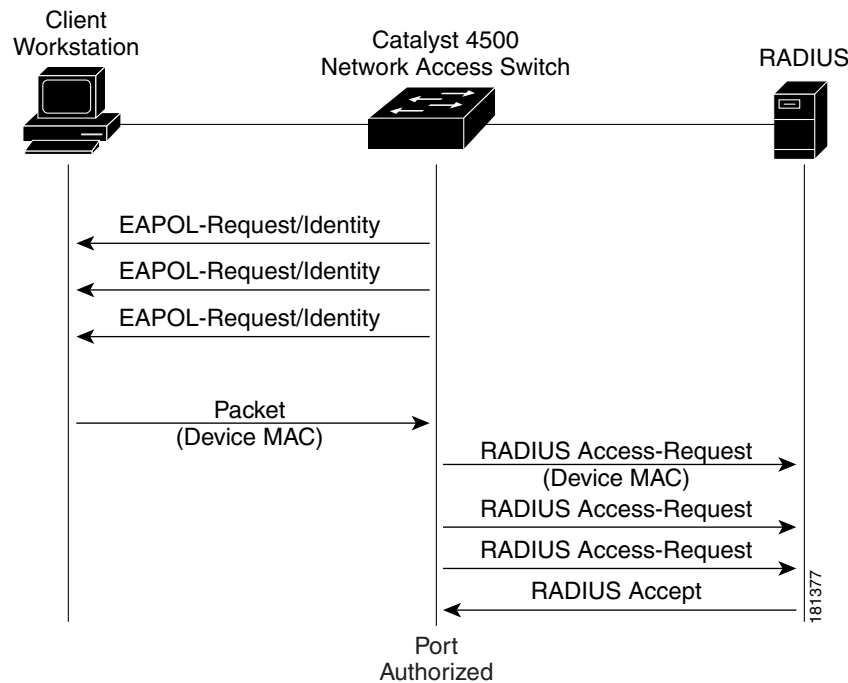
Based on the default 802.1X timer values, the transition between mechanisms takes approximately 90 seconds. You can shorten the time by reducing the value of the transmission period time, which affects the frequency of EAPOL transmission. A smaller timer value results in EAPOLs sent during a shorter period of time. With MAB enabled, after 802.1X performs one full set of EAPOLs, the learned MAC address is forwarded to the authentication server for processing.

The MAB module performs authorization for the first MAC address detected on the wire. The port is considered authorized once a valid MAC address is received that RADIUS approves of.

802.1X authentication can re-start if an EAPOL packet is received on a port that was initially authorized as a result of MAB.

[Figure 37-5](#) shows the message exchange during MAB.

Figure 37-5 Message Exchange during MAC Authentication Bypass



- The authentication-failed VLAN is used only with dot1x-authentication-failed users. MAB is not attempted with dot1x-authentication-failed users. If 802.1X authentication fails, a port moves to the authentication-failed VLAN (if configured) whether MAB is configured or not.
- When both MAB and guest VLAN are configured and no EAPOL packets are received on a port, the 802.1X state-machine is moved to a MAB state where it opens the port to listen to traffic and grab MAC addresses. The port remains in this state forever waiting to see a MAC on the port. A detected MAC address that fails authorization causes the port to be moved to the guest VLAN if configured.

While in a guest VLAN, a port is open to all traffic on the specified guest VLAN. Therefore, non-802.1X supplicants that normally would be authorized but are in guest VLAN due to the earlier detection of a device that failed authorization, would remain in the guest VLAN indefinitely. However, loss of link or the detection of an EAPOL on the wire causes a transition out of the guest VLAN and back to the default 802.1X mode.

- Once a new MAC has been authenticated by MAB, the responsibility to limit access falls upon the 802.1X Authenticator (or port security) to secure the port. The 802.1X default host parameter is defined only for a single host. If the port is changed to multi-user host, port security must be employed to enforce the number of MAC addresses allowed thru this port.

- Catalyst 4500 series switch supports MAB with VVID, with the restriction that the MAC address appears on a port data VLAN only. All IP phone MACs learned via CDP are allowed on voice VLANs.
- MAB and VMPS are mutually exclusive because their functionality overlaps.

Using 802.1X with Inaccessible Authentication Bypass

**Note**

Supervisor Engine 6-E does *not* support this feature.

When a switch cannot reach the configured RADIUS servers and clients (suplicants) cannot be authenticated, you can configure a switch to allow network access to hosts connected to *critical* ports that are enabled for Inaccessible Authentication Bypass.

When this feature is enabled, a switch monitors the status of the configured RADIUS servers. If no RADIUS servers are available, ports with Inaccessible Authentication Bypass enabled are authorized. You can specify a Inaccessible Authentication Bypass VLAN on a per-port basis.

Ports that were already authorized when RADIUS becomes unavailable are unaffected by Inaccessible Authentication Bypass. However, if re-authentication is applied and RADIUS is not restored by the next polling cycle, ports already authorized falls back to the critical auth VLAN.

When RADIUS becomes available, critically-authorized ports may be configured to automatically reauthenticate themselves.

For details on how to configure Inaccessible Authentication Bypass, see the [“Configuring 802.1X with Inaccessible Authentication Bypass”](#) section on page 37-36.

Using 802.1X with Unidirectional Controlled Port

**Note**

Supervisor Engine 6-E does *not* support this feature.

Unidirectional Controlled Port is a combined hardware/software feature that allows dormant PCs to be “powered on” based on the receipt of a specific Ethernet frame, known as the *magic packet*. Generally, Unidirectional Controlled Port is used in environments where administrators plan to manage remote systems during off-hours, when it’s likely that the systems have been powered down.

Use of Unidirectional Controlled Port with hosts attached through 802.1X ports presents a unique problem; when the host powers down, a 802.1X port becomes unauthorized. In this state, the port allows the receipt and transmission of EAPoL packets only. Therefore, the Unidirectional Controlled Port magic packet cannot reach the host; without powering up, the PC cannot authenticate and open the port.

Unidirectional Controlled Port solves this problem by allowing packets to be transmitted on unauthorized 802.1X ports.

**Note**

Unidirectional Controlled Port only works when Spanning Tree Portfast is enabled on the port.

For details on how to configure 802.1X with Unidirectional Controlled Port, see the [“Configuring 802.1X with Unidirectional Controlled Port”](#) section on page 37-39

Unidirectional State

When you configure a port as unidirectional with the **dot1x control-direction in** interface configuration command, the port changes to the spanning-tree forwarding state.

When Unidirectional Controlled Port is enabled, the connected host is in the sleeping mode or power-down state. The host does not exchange traffic with other devices in the network. If the host connected to the unidirectional port that cannot send traffic to the network, the host can only receive traffic from other devices in the network.

Bidirectional State

When you configure a port as bidirectional with the **dot1x control-direction both** interface configuration command, the port is access-controlled in both directions. In this state, except EAPOL packets, the switch port does not receive or send packets.

Using 802.1X with Authentication Failed VLAN Assignment

**Note**

Supervisor Engine 6-E does *not* support this feature.

You can use authentication-failed VLAN assignment on a per-port basis to provide access for authentication failed users. Authentication failed users are end hosts that are 802.1X- capable but do not have valid credentials in an authentication server or end hosts that do not give any username and password combination in the authentication pop-up window on the user side.

If a user fails the authentication process, that port is placed in the authentication-failed VLAN. The port remains in the authentication-failed VLAN until the reauthentication timer expires. When the reauthentication timer expires the switch starts sending the port re-authentication requests. If the port fails reauthentication it remains in the authentication-failed VLAN. If the port is successfully reauthenticated, the port is moved either to the VLAN sent by RADIUS server or to the newly authenticated ports configured VLAN; the location depends on whether RADIUS is configured to send VLAN information.

**Note**

When enabling periodic reauthentication (see the [“Enabling Periodic Reauthentication”](#) section on page 37-42), only local reauthentication timer values are allowed. You cannot utilize a RADIUS server to assign the reauthentication timer value.

You can set the maximum number of authentication attempts that the authenticator sends before moving a port into the authentication-failed VLAN. The authenticator keeps a count of the failed authentication attempts for each port. A failed authentication attempt is either an empty response or an EAP failure. The authenticator tracks any mix of failed authentication attempts towards the authentication attempt count. After the maximum number of attempts is reached the port is placed in the authentication-failed VLAN until the reauthentication timer expires again.

**Note**

RADIUS may send a response without an EAP packet in it when it does not support EAP, and sometimes third party RADIUS servers also send empty responses. When this happens, the authentication attempt counter is incremented.

For details on how to configure Authentication Failed VLAN Assignment, see the [“Configuring 802.1X with Authentication Failed VLAN Assignment”](#) section on page 37-40.

Usage Guidelines for Using Authentication Failed VLAN Assignment

- You should enable reauthentication. The ports in authentication-failed VLANs do not receive reauthentication attempts if reauthentication is disabled. In order to start the reauthentication process the authentication-failed VLAN must receive a link down event or an EAP logoff event from the port. If the host is behind a hub, you may never get a link down event and may not detect the new host until the next reauthentication occurs. Therefore, it is recommended to have re-authentication enabled in that case.
- EAP failure messages are not sent to the user. If the user fails authentication the port is moved to an authentication-failed VLAN and a EAP success message is sent to the user. Because the user is not notified of the authentication failure there may be confusion as to why there is restricted access to the network. A EAP Success message is sent for the following reasons:
 - If the EAP Success message is not sent, the user tries to authenticate every 60 seconds (by default) by sending an EAP-start message.
 - In some cases, users have configured DHCP to EAP-Success and unless the user sees a success, DHCP does not work on the port.
- Sometimes a user caches an incorrect username and password combination after receiving a EAP success message from the authenticator and reuses that information in every re-authentication. Until the user passes the correct username and password combination the port remains in the authentication-failed VLAN.
- When an authentication failed port is moved to an unauthorized state the authentication process is restarted. If you should fail the authentication process again the authenticator waits in the held state. After you have correctly reauthenticated all 802.1X ports are reinitialized and treated as normal 802.1X ports.
- When you reconfigure an authentication-failed VLAN to a different VLAN, any authentication failed ports are also moved and the ports stay in their current authorized state.
- When you shut down or remove an authentication-failed VLAN from the VLAN database, any authentication failed ports are immediately moved to an unauthorized state and the authentication process is restarted. The authenticator does not wait in a held state because the authentication-failed VLAN configuration still exists. While the authentication-failed VLAN is inactive, all authentication attempts are counted, and as soon as the VLAN becomes active the port is placed in the authentication-failed VLAN.
- If you reconfigure the maximum number of authentication failures allowed by the VLAN, the change takes affect after the reauthentication timer expires.
- All internal VLANs which are used for Layer 3 ports cannot be configured as an authentication-failed VLAN.
- The authentication-failed VLAN is supported only in single-host mode (the default port mode).
- When a port is placed in an authentication-failed VLAN the user’s MAC address is added to the mac-address-table. If a new MAC address appears on the port, it is treated as a security violation.
- When an authentication failed port is moved to an authentication-failed VLAN, the Catalyst 4500 series switch does not transmit a RADIUS-Account Start Message like it does for regular 802.1X authentication.

Using 802.1X with Port Security

You can enable port security on an 802.1X port in either single- or multiple-host mode. (To do so, you must configure port security with the **switchport port-security** interface configuration command. Refer to the nb chapter in this guide.) When you enable port security and 802.1X on a port, 802.1X authenticates the port, and port security manages the number of MAC addresses allowed on that port, including that of the client. Hence, you can use an 802.1X port with port security enabled to limit the number or group of clients that can access the network.

For information on selecting multi-host mode, see the [“Resetting the 802.1X Configuration to the Default Values” section on page 37-48](#).

These examples describe the interaction between 802.1X and port security on a switch:

- When a client is authenticated, and the port security table is not full, the client’s MAC address is added to the port security list of secure hosts. The port then proceeds to come up normally.

When a client is authenticated and manually configured for port security, it is guaranteed an entry in the secure host table (unless port security static aging has been enabled).

A security violation occurs if an additional host is learned on the port. The action taken depends on which feature (802.1X or port security) detects the security violation:

- If 802.1X detects the violation, the action is to err-disable the port.
- If port security detects the violation, the action is to shutdown or restrict the port (the action is configurable).

The following describes when port security and 802.1X security violations occur:

- In single host mode, after the port is authorized, any MAC address received other than the client’s causes a 802.1X security violation.
- In single host mode, if installation of an 802.1X client’s MAC address fails because port security has already reached its limit (due to a configured secure MAC addresses), a port security violation is triggered.
- In multi host mode, once the port is authorized, any additional MAC addresses that cannot be installed because the port security has reached its limit triggers a port security violation.
- When an 802.1X client logs off, the port transitions back to an unauthenticated state, and all dynamic entries in the secure host table are cleared, including the entry for the client. Normal authentication then ensues.
- If you administratively shut down the port, the port becomes unauthenticated, and all dynamic entries are removed from the secure host table.
- Only 802.1X can remove the client’s MAC address from the port security table. Note that in multi host mode, with the exception of the client’s MAC address, all MAC addresses that are learned by port security can be deleted using port security CLIs.
- Whenever port security ages out a 802.1X client’s MAC address, 802.1X attempts to reauthenticate the client. Only if the reauthentication succeeds is the client’s MAC address be retained in the port security table.
- All of the 802.1X client’s MAC addresses are tagged with (dot1x) when you display the port security table by using CLI.

Using 802.1X with RADIUS-Provided Session Timeouts

You can specify whether a switch uses a locally configured or a RADIUS-provided reauthentication timeout. If the switch is configured to use the local timeout, it reauthenticates the host when the timer expires.

If the switch is configured to use the RADIUS-provided timeout, it looks in the RADIUS Access-Accept message for the Session-Timeout and optional Termination-Action attributes. The switch uses the value of the Session-Timeout attribute to determine the duration of the session, and it uses the value of the Termination-Action attribute to determine the switch action when the session's timer expires.

If the Termination-Action attribute is present and its value is RADIUS-Request, the switch reauthenticates the host. If the Termination-Action attribute is not present, or its value is Default, the switch terminates the session.



Note

The supplicant on the port detects that its session has been terminated and attempts to initiate a new session. Unless the authentication server treats this new session differently, the client may see only a brief interruption in network connectivity as the switch sets up a new session.

If the switch is configured to use the RADIUS-supplied timeout, but the Access-Accept message does not include a Session-Timeout attribute, the switch never reauthenticates the supplicant. This behavior is consistent with Cisco's wireless access points.

For details on how to configure RADIUS-provided session timeouts, see the [“Configuring RADIUS-Provided Session Timeouts”](#) section on page 37-31.

Using 802.1X with RADIUS Accounting



Note

Supervisor Engine 6-E does *not* support this feature.



Note

If you plan to implement system-wide accounting, you should also configure 802.1X accounting. Moreover, you need to inform the accounting server of the system reload event when the system is reloaded. Doing this ensures that the accounting server is aware that all outstanding 802.1X sessions on this system are closed.



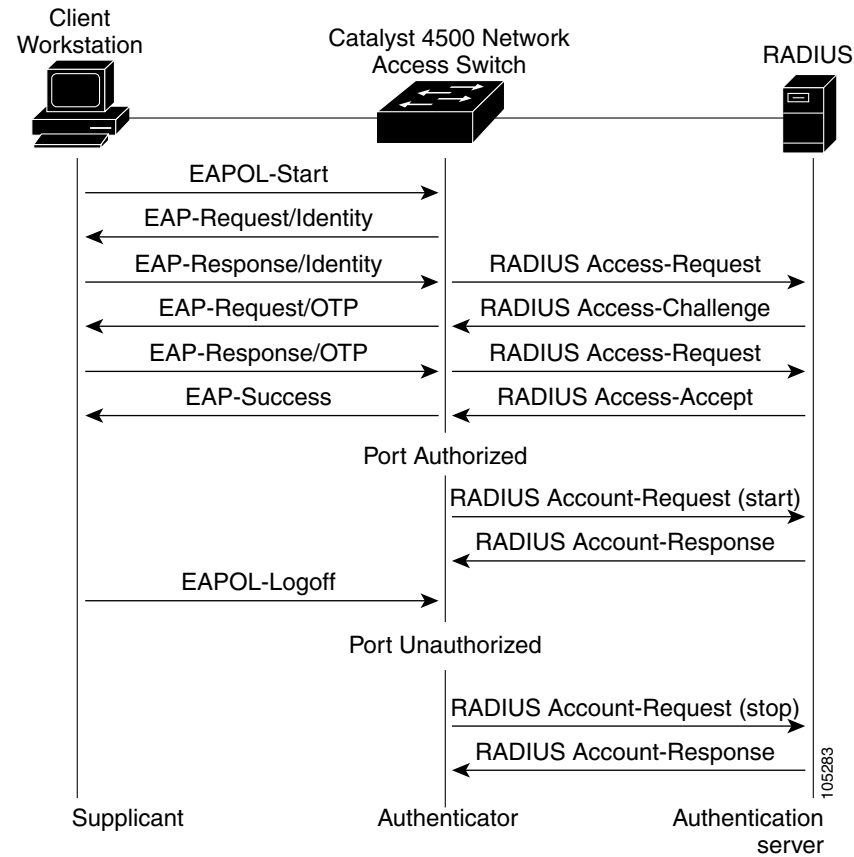
Note

To enable 802.1X accounting, you must first configure 802.1X authentication and switch-to-RADIUS server communication.

802.1X RADIUS accounting relays important events to the RADIUS server (such as the client's connection session). This session is defined as the interval beginning when the client is authorized to use the port and ending when the client stops using the port.

[Figure 37-6](#) illustrates the RADIUS accounting process.

Figure 37-6 RADIUS Accounting

**Note**

You must configure the 802.1X client to send an EAP-logoff (Stop) message to the switch when the user logs off. If you do not configure the 802.1X client, an EAP-logoff message is not sent to the switch and the accompanying accounting Stop message is not sent to the authentication server. Refer to the Microsoft Knowledge Base article at the location: <http://support.microsoft.com>. Also refer to the Microsoft article at this location:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0703.asp>,

and set the SupplicantMode registry to 3 and the AuthMode registry to 1.

After the client is authenticated, the switch sends accounting-request packets to the RADIUS server, which responds with accounting-response packets to acknowledge the receipt of the request.

A RADIUS accounting-request packet contains one or more Attribute-Value pairs to report various events and related information to the RADIUS server. The following events are tracked:

- User successfully authenticates
- User logs-off
- Link-down occurs on a 802.1X port
- Reauthentication succeeds
- Reauthentication fails

When the port state transitions between authorized and unauthorized, the RADIUS messages are transmitted to the RADIUS server.

The switch does not log any accounting information. Instead, it sends such information to the RADIUS server, which must be configured to log accounting messages.

The 802.1X authentication, authorization and accounting process is as follows:

-
- Step 1** A user connects to a port on the switch.
 - Step 2** Authentication is performed, for example, using the username/password method.
 - Step 3** VLAN assignment is enabled, as appropriate, per RADIUS server configuration.
 - Step 4** The switch sends a start message to an accounting server.
 - Step 5** Reauthentication is performed, as necessary.
 - Step 6** The switch sends an interim accounting update to the accounting server that is based on the result of reauthentication.
 - Step 7** The user disconnects from the port.
 - Step 8** The switch sends a stop message to the accounting server.
-

To configure 802.1X accounting, you need to do the following tasks:

- Enable logging of “Update/Watchdog packets from this AAA client” in your RADIUS server’s Network Configuration tab.
- Enable “Logging>CVS RADIUS Accounting” in your RADIUS server System Configuration tab.
- Enable 802.1X accounting on your switch.
- Enable AAA accounting by using the **aaa system accounting** command. Refer to the [“Enabling 802.1X RADIUS Accounting”](#) section on page 37-32.

Enabling AAA system accounting along with 802.1X accounting allows system reload events to be sent to the accounting RADIUS server for logging. By doing this, the accounting RADIUS server can infer that all active 802.1X sessions are appropriately closed.

Because RADIUS uses the unreliable transport protocol UDP, accounting messages may be lost due to poor network conditions. If the switch does not receive the accounting response message from the RADIUS server after a configurable number of retransmissions of an accounting request, the following system message appears:

```
Accounting message %s for session %s failed to receive Accounting Response.
```

When the stop message is not transmitted successfully, a message like the following appears:

```
00:09:55: %RADIUS-3-NOACCOUNTINGRESPONSE: Accounting message Start for session
172.20.50.145 sam 11/06/03 07:01:16 11000002 failed to receive Accounting Response.
```

Use the **show radius statistics** command to display the number of RADIUS messages that do not receive the accounting response message.

Using 802.1X with Voice VLAN Ports

A voice VLAN port is a special access port associated with two VLAN identifiers:

- Voice VLAN ID (VVID) to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.
- Port VLAN ID (PVID) to carry the data traffic to and from the workstation connected to the switch through the IP phone. The PVID is the native VLAN of the port.

Each port that you configure for a voice VLAN is associated with a VVID and a PVID. This configuration allows voice traffic and data traffic to be separated onto different VLANs.

A voice VLAN port becomes active when there is a link whether or not the port is AUTHORIZED or UNAUTHORIZED. All traffic coming through the voice VLAN is learned correctly and appears in the MAC-address-table. Cisco IP phones do not relay CDP messages from other devices. As a result, if several Cisco IP phones are connected in series, the switch recognizes only the one directly connected to it. When 802.1X is enabled on a voice VLAN port, the switch drops packets from unrecognized Cisco IP phones more than one hop away.

When 802.1X is enabled on a port, you cannot configure a PVID that is equal to a VVID. For more information about voice VLANs, see [Chapter 33, “Configuring Voice Interfaces.”](#)

Be aware of the following feature interactions:

- 802.1X VLAN assignment cannot assign to the port the same VLAN as the voice VLAN; otherwise, the 802.1X authentication fails.
- 802.1X guest VLAN works with the 802.1X voice VLAN port feature. However, the guest VLAN cannot be the same as the voice VLAN.
- 802.1X port security works with the 802.1X voice VLAN port feature and is configured per port. Two MAC addresses must be configured: one for the Cisco IP phone MAC address on the VVID and one for the PC MAC-address on PVID.

However, you cannot use the 802.1X voice VLAN port feature with 802.1X port security’s sticky MAC address configuration and statically configured MAC address configuration.

- 802.1X accounting is unaffected by the 802.1X voice VLAN port feature.
- When 802.1X is configured on a port, you cannot connect multiple IP-phones to a Catalyst 4500 series switch through a hub.
- Because voice VLANs cannot be configured as private VLAN host ports, and because only private VLANs can be assigned to private VLAN host ports, VLAN assignment cannot assign a private VLAN to a port with a voice VLAN configured.

For details on how to configure 802.1X with voice VLANs, see the [“Configuring 802.1X with Voice VLAN” section on page 37-41.](#)

Using Multiple Domain Authentication

Multiple Domain Authentication (MDA) allows both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port, which is divided into a data domain and a voice domain.

MDA does not enforce the order of device authentication. For best results, however, you should authenticate a voice device before you authenticate a data device on an MDA-enabled port.

Observe the following guidelines for configuring MDA:

- **It is highly recommended that you enable CoPP on an MDA-enabled port to protect against a DoS attack. Refer to [Chapter 39, “Configuring Control Plane Policing.”](#)**
- To configure a switch port for MDA, see the [“Configuring Multiple Domain Authentication” section on page 37-28.](#)
- You must configure the voice VLAN for the IP phone when the host mode is set to multidomain. For more information, see [Chapter 33, “Configuring Voice Interfaces.”](#)



Note If you use a dynamic VLAN to assign a voice VLAN on an MDA-enabled switch port, the voice device fails authorization.

- To authorize a voice device, the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of `device-traffic-class=voice`. Without this value, the switch treats the voice device as a data device.
- The guest VLAN and restricted VLAN features only apply to the data devices on an MDA-enabled port. The switch treats a voice device that fails authorization as a data device.
- If more than one device attempts authorization on either the voice or the data domain of a port, it is error disabled.
- Until a device is authorized, the port drops its traffic. Non-Cisco IP phones or voice devices are allowed into both the data and voice VLANs. The data VLAN allows the voice device to contact a DHCP server to obtain an IP address and acquire the voice VLAN information. After the voice device starts sending on the voice VLAN, its access to the data VLAN is blocked.
- You can use dynamic VLAN assignment from a RADIUS server only for data devices.
- MDA can use MAC authentication bypass as a fallback mechanism to allow the switch port to connect to devices that do not support 802.1X authentication. This is especially useful for 3rd-party phones without 802.1X supplicant. For more information, see the [“Using 802.1X with MAC Authentication Bypass” section on page 37-9.](#)
- When a *data* or a *voice* device is detected on a port, its MAC address is blocked until authorization succeeds. If the authorization fails, the MAC address remains blocked for 5 minutes.
- If more than one device is detected on the *data* VLAN or more than one voice device is detected on the *voice* VLAN while a port is unauthorized, the port is error disabled.
- When a port host mode is changed from single- or multihost to multidomain mode, an authorized data device remains authorized on the port. However, a Cisco IP phone that has been allowed on the port in the voice VLAN is automatically removed and must be reauthenticated on that port.
- Active fallback mechanisms such as guest VLAN and restricted VLAN remain configured after a port changes from single- or multihost mode to multidomain mode.
- Switching a port host mode from multidomain to single- or multihost mode removes all authorized devices from the port.
- If a data domain is authorized first and placed in the guest VLAN, non-802.1X-capable voice devices need to tag their packets on the voice VLAN to trigger authentication.
- We do not recommend per-user ACLs with an MDA-enabled port. An authorized device with a per-user ACL policy might impact traffic on both the voice and data VLANs of the port. If used, only one device on the port should enforce per-user ACLs.

Supported Topologies

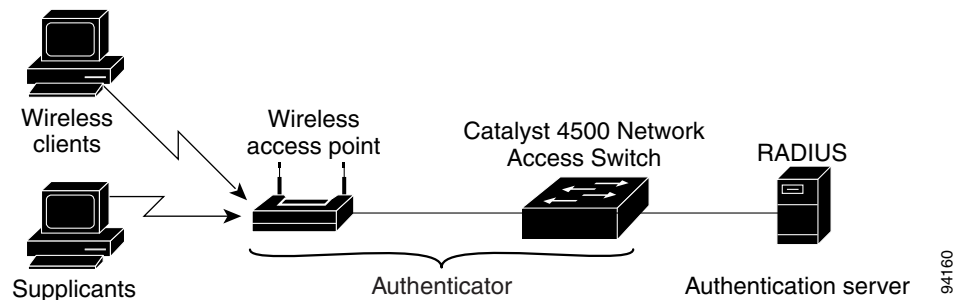
The 802.1X port-based authentication supports two topologies:

- Point to point
- Wireless LAN

In a point-to-point configuration (see [Figure 37-1 on page 37-2](#)), only one client can be connected to the 802.1X-enabled switch port when the multi-host mode is not enabled (the default). The switch detects the client when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

For 802.1X port-based authentication in a wireless LAN ([Figure 37-7](#)), you must configure the 802.1X port as a multiple-host port that is authorized as a wireless access point once the client is authenticated. (See the [“Resetting the 802.1X Configuration to the Default Values”](#) section on page 37-48.) When the port is authorized, all other hosts that are indirectly attached to the port are granted access to the network. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the switch denies access to the network for all wireless access point-attached clients. In this topology, the wireless access point is responsible for authenticating clients attached to it, and the wireless access point acts as a client to the switch.

Figure 37-7 Wireless LAN Example



Configuring 802.1X

To configure 802.1X, follow this procedure:

-
- Step 1** Enable 802.1X authentication. See the [“Enabling 802.1X Authentication”](#) section on page 37-23.
 - Step 2** Configure switch to RADIUS server communication. See the [“Configuring Switch-to-RADIUS-Server Communication”](#) section on page 37-26.
 - Step 3** Adjust the 802.1X timer values. See the [“Changing the Quiet Period”](#) section on page 37-44.
 - Step 4** Configure optional features. See the [“Configuring RADIUS-Provided Session Timeouts”](#) section on page 37-31.
-

These sections describe how to configure 802.1X:

- [Default 802.1X Configuration, page 37-22](#)
- [802.1X Configuration Guidelines, page 37-23](#)
- [Enabling 802.1X Authentication, page 37-23 \(required\)](#)
- [Configuring Switch-to-RADIUS-Server Communication, page 37-26 \(required\)](#)
- [Configuring Multiple Domain Authentication, page 37-28](#)
- [Configuring RADIUS-Provided Session Timeouts, page 37-31 \(optional\)](#)
- [Enabling 802.1X RADIUS Accounting, page 37-32 \(optional\)](#)
- [Configuring 802.1X with Guest VLANs, page 37-32 \(optional\)](#)
- [Configuring 802.1X with MAC Authentication Bypass, page 37-35 \(optional\)](#)
- [Configuring 802.1X with Inaccessible Authentication Bypass, page 37-36 \(optional\)](#)
- [Configuring 802.1X with Unidirectional Controlled Port, page 37-39 \(optional\)](#)
- [Configuring 802.1X with Authentication Failed VLAN Assignment, page 37-40 \(optional\)](#)
- [Configuring 802.1X with Voice VLAN, page 37-41 \(optional\)](#)
- [Enabling Periodic Reauthentication, page 37-42 \(optional\)](#)
- [Enabling Multiple Hosts, page 37-43 \(optional\)](#)
- [Changing the Quiet Period, page 37-44 \(optional\)](#)
- [Changing the Switch-to-Client Retransmission Time, page 37-45 \(optional\)](#)
- [Setting the Switch-to-Client Frame-Retransmission Number, page 37-46 \(optional\)](#)
- [Manually Reauthenticating a Client Connected to a Port, page 37-47 \(optional\)](#)
- [Initializing the 802.1X Authentication State, page 37-47](#)
- [Removing 802.1X Client Information, page 37-48](#)
- [Resetting the 802.1X Configuration to the Default Values, page 37-48 \(optional\)](#)

Default 802.1X Configuration

Table 37-1 shows the default 802.1X configuration.

Table 37-1 Default 802.1X Configuration

Feature	Default Setting
Authentication, authorization, and accounting (AAA)	Disabled
RADIUS server <ul style="list-style-type: none"> • IP address • UDP authentication port • Key 	<ul style="list-style-type: none"> • None specified • 1812 • None specified
Per-interface 802.1X protocol enable state	Force-authorized The port transmits and receives normal traffic without 802.1X-based authentication of the client.

Table 37-1 Default 802.1X Configuration (continued)

Feature	Default Setting
Periodic reauthentication	Disabled
Time between reauthentication attempts	3600 sec
Quiet period	60 sec Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.
Retransmission time	30 sec Number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before retransmitting the request.
Maximum retransmission number	2 Number of times that the switch sends an EAP-request/identity frame before restarting the authentication process.
Multiple host support	Disabled
Client timeout period	30 sec When relaying a request from the authentication server to the client, the amount of time that the switch waits for a response before retransmitting the request to the client.
Authentication server timeout period	30 sec When relaying a response from the client to the authentication server, the amount of time that the switch waits for a reply before retransmitting the response to the server. This setting is not configurable.

802.1X Configuration Guidelines

This section describes the guidelines for configuring 802.1X authentication:

- The 802.1X Protocol is supported only on Layer 2 static access, private VLAN host ports, and Layer 3 routed ports. You cannot configure 802.1X for any other port modes.
- If you are planning to use either 802.1X accounting or VLAN assignment, be aware that both features utilize general AAA commands. For information on how to configure AAA, refer to the “Enabling 802.1X Authentication” section on page 37-23. Alternatively, you can refer to the Cisco IOS security documentation:
 - http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fsecur_c/index.htm
 - http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fsecur_r/index.htm

Enabling 802.1X Authentication

To enable 802.1X port-based authentication, you first must enable 802.1X globally on your switch, then enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods that must be queried to authenticate a user.

The software uses the first method listed in the method list to authenticate users; if that method fails to respond, the software selects the next authentication method in the list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

**Note**

To allow VLAN assignment, you must enable AAA authorization to configure the switch for all network-related service requests.

To configure 802.1X port-based authentication, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# dot1x system-auth-control	Enables 802.1X on your switch. To disable 802.1X globally on the switch, use the no dot1x system-auth-control command.
Step 3	Switch(config)# aaa new-model	Enables AAA. To disable AAA, use the no aaa new-model command.
Step 4	Switch(config)# aaa authentication dot1x {default} method1 [method2...]	Creates an 802.1X AAA authentication method list. To create a default list that is used when a named list is not specified in the authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. Enter at least one of these keywords: <ul style="list-style-type: none"> • group radius—Use the list of all RADIUS servers for authentication. • none—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client. To disable 802.1X AAA authentication, use the no aaa authentication dot1x {default list-name} method1 [method2...] global configuration command.
Step 5	Switch(config)# aaa authorization network {default} group radius	(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as VLAN assignment.
Step 6	Switch(config)# interface interface-id	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 7	Switch(config-if)# switchport mode access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 8	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “ Default 802.1X Configuration ” section on page 37-22.
Step 9	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 10	Switch(config-if)# end	Returns to privileged EXEC mode.

	Command	Purpose
Step 11	Switch # show dot1x interface interface-id details	Verifies your entries. Check the PortControl row in the 802.1X port summary section of this display. The PortControl value is set to auto .
Step 12	Switch# show running-config	Verifies your entries.
Step 13	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.



Note Enabling Spanning Tree PortFast ensures that a port comes up immediately after authorization.



Note Whenever you configure any 802.1X parameter on a port, a dot1x authenticator is automatically created on the port. As a result **dot1x pae authenticator** appears in the configuration. This is to ensure that dot1x authentication still works on legacy configurations without manual intervention. This is likely to change in future releases.

This example shows how to enable 802.1X and AAA on Fast Ethernet port 2/1, and how to verify the configuration:

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# interface fastethernet2/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch# show dot1x interface f7/1 details
```

```
Dot1x Info for FastEthernet7/1
-----
PAE                               = AUTHENTICATOR
PortControl                        = AUTO
ControlDirection                  = Both
HostMode                           = SINGLE_HOST
ReAuthentication                   = Disabled
QuietPeriod                        = 60
ServerTimeout                     = 30
SuppTimeout                       = 30
ReAuthPeriod                       = 3600 (Locally configured)
ReAuthMax                          = 2
MaxReq                             = 2
TxPeriod                          = 30
RateLimitPeriod                   = 0
```

```
Dot1x Authenticator Client List
-----
Supplicant                        = 1000.0000.2e00
    Auth SM State                  = AUTHENTICATED
    Auth BEND SM Stat              = IDLE
Port Status                       = AUTHORIZED
```

```
Authentication Method    = Dot1x
Authorized By           = Authentication Server
Vlan Policy              = N/A
```

Configuring Switch-to-RADIUS-Server Communication

A RADIUS security server is identified by its host name or IP address, host name and specific UDP port number, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order they were configured.

To configure the RADIUS server parameters on the switch, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# radius-server host {hostname ip-address} auth-port port-number [acct-port port-number] [test username name] [ignore-auth-port] [ignore-acct-port] [idle-time min] key string	<p>Configures the RADIUS server parameters on the switch.</p> <p>For <i>hostname</i> <i>ip-address</i>, specify the hostname or IP address of the remote RADIUS server.</p> <p>To delete the specified RADIUS server, use the no radius-server host {<i>hostname</i> <i>ip-address</i>} global configuration command.</p> <p>The auth-port <i>port-number</i> specifies the UDP destination port for authentication requests. The default is 1812.</p> <p>The acct-port <i>port-number</i> specifies the UDP destination port for accounting requests. The default is 1813.</p> <p>Use test username <i>name</i> to enable automated RADIUS server testing, and to detect the RADIUS server going up and down. The name parameter is the username used in the test access request sent to the RADIUS server; it does not need to be a valid user configured on the server. The ignore-auth-port and ignore-acct-port options disable testing on the authentication and accounting ports respectively.</p> <p>The idle-time <i>min</i> parameter specifies the number of minutes before an idle RADIUS server is tested to verify that it is still up. The default is 60 minutes.</p> <p>The key <i>string</i> specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server.</p> <p>Note Always configure the key as the last item in the radius-server host command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.</p> <p>If you want to use multiple RADIUS servers, use this command multiple times.</p>
Step 3	Switch(config-if)# radius deadtime min	(Optional) Configures the number of minutes before a dead RADIUS server is tested to check whether it has come back up. The default is 1 minute.
Step 4	Switch(config-if)# radius dead-criteria time seconds tries num	<p>(Optional) Configures the criteria used to decide whether a RADIUS server is dead. The time parameter specifies the number of seconds after which a request to the server is unanswered before it is considered dead. The tries parameter specifies the number of times a request to the server is unanswered before it is considered dead.</p> <p>The recommended values for these parameters are tries equal to radius-server retransmit and time equal to radius-server retransmit x radius-server timeout.</p>

	Command	Purpose
Step 5	Switch(config-if)# ip radius source-interface m/p	Establishes the IP address to be used as the source address for all outgoing RADIUS packets.
Step 6	Switch(config)# end	Returns to privileged EXEC mode.
Step 7	Switch# show running-config	Verifies your entries.
Step 8	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to specify the server with IP address 172.120.39.46 as the RADIUS server. The first command specifies port 1612 as the authorization port, sets the encryption key to rad123.

The second command dictates that key matches are performed on the RADIUS server:

```
Switch# configure terminal
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
Switch(config)# ip radius source-interface m/p
Switch(config)# end
Switch#
```

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, **radius-server retransmit**, and the **radius-server key** global configuration commands.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch.

Configuring Multiple Domain Authentication

To configure MDA, perform these steps.

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# radius-server vsa send authentication	Configures the network access server to recognize and use vendor-specific attributes (VSAs).
Step 3	Switch(config)# interface interface-id	Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode.

	Command	Purpose
Step 4	Switch(config-if)# [no] dot1x host-mode {single-host multi-host multi-domain}	<p>The keywords have these meanings:</p> <ul style="list-style-type: none"> • single-host—Allow a single host (client) on an IEEE 802.1X-authorized port. • multi-host—Allow multiple hosts on an 802.1X-authorized port after a single host has been authenticated. • multi-domain—Allow both a host and a voice device, such as an IP phone (Cisco or non-Cisco), to be authenticated on an IEEE 802.1X-authorized port. <p>Note You must configure the voice VLAN for the IP phone when the host mode is set to multi-domain. For more information, see Chapter 33, “Configuring Voice Interfaces.”</p> <p>Ensure that the dot1x port-control interface configuration command is set to auto for the specified interface.</p> <p>To disable multiple hosts on the port, use the no dot1x host-mode multi-host interface configuration command.</p>
Step 5	Switch(config-if)# switchport voice vlan <i>vlan-id</i>	(Optional) Configures the voice VLAN.
Step 6	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 7	Switch# show dot1x interface <i>interface-id</i> [detail]	Verifies your entries.
Step 8	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to enable 802.1X authentication and to allow multiple hosts:

```
Switch(config)# interface gigabitEthernet2/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
Switch(config-if)# end
```

This example shows how to enable MDA and to allow both a host and a 802.1X voice device (e.g., a Cisco or 3rd-party phone with 802.1X supplicant) on the port:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# no shut
Switch(config-if)# end
```

This example shows how to enable MDA and to allow both a host and a non-802.1X voice device on the port:

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface FastEthernet3/1
Switch(config-if)# shut
Switch(config-if)# switchport access vlan 12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-domain
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)# no shut
Switch(config-if)# end
```

This example shows how to verify the dot1x MDA settings on interface FastEthernet6/1:

```
Switch# show dot1x interface FastEthernet3/1 detail

Dot1x Info for FastEthernet3/1
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = MULTI_DOMAIN
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

Dot1x Authenticator Client List
-----
Domain = DATA
Supplicant = 0000.0000.ab01
    Auth SM State = AUTHENTICATED
    Auth BEND SM Stat = IDLE
Port Status = AUTHORIZED
Authentication Method = Dot1x
Authorized By = Authentication Server
Vlan Policy = 12

Domain = VOICE
Supplicant = 0060.b057.4687
    Auth SM State = AUTHENTICATED
    Auth BEND SM Stat = IDLE
Port Status = AUTHORIZED
Authentication Method = Dot1x
Authorized By = Authentication Server

Switch#
```

Configuring RADIUS-Provided Session Timeouts

You can configure the Catalyst 4500 series switch to use a RADIUS-provided reauthentication timeout. To configure RADIUS-provided timeouts, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface interface-id	Enters interface configuration mode.
Step 3	Switch(config-if)# switchport mode access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “Default 802.1X Configuration” section on page 37-22.
Step 5	Switch(config-if)# dot1x timeout reauth-period {interface server}	Sets the re-authentication period (seconds).
Step 6	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 7	Switch# show dot1x interface interface-id details	Verifies your entries.
Step 8	Switch # copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to configure the switch to derive the re-authentication period from the server and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface f7/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout reauth-period server
Switch(config-if)# end
Switch# show dot1x interface f7/1 det

Dot1x Info for FastEthernet7/11
-----
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = (From Authentication Server)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0

Dot1x Authenticator Client List Empty

Port Status = AUTHORIZED

Switch#
```

Enabling 802.1X RADIUS Accounting



Note Supervisor Engine 6-E does *not* support this feature.

To configure 802.1X accounting, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# aaa accounting dot1x default start-stop group radius	Enables 802.1X accounting, using the list of all RADIUS servers.
Step 3	Switch(config)# clock timezone PST -8	Sets the time zone for the accounting event-time stamp field.
Step 4	Switch(config)# clock calendar-valid	Enables the date for the accounting event-time stamp field.
Step 5	Switch(config)# aaa accounting system default start-stop group radius	(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.
Step 6	Switch(config)# end	Returns to privileged EXEC mode.
Step 7	Switch# show running-config	Verifies your entries.
Step 8	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to specify the server with IP address 172.120.39.46 as the RADIUS server. The first command configures the RADIUS server, specifying port 1612 as the authorization port, 1813 as the UDP port for accounting, and rad123 as the encryption key:

```
Switch# configure terminal
Switch(config)# radius-server host 172.120.39.46 auth-port 1812 acct-port 1813 key rad123
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting system default start-stop group radius
Switch(config)# end
Switch#
```



Note You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps. To turn on these functions, enable logging of “Update/Watchdog packets from this AAA client” in your RADIUS server Network Configuration tab. Next, enable “CVS RADIUS Accounting” in your RADIUS server System Configuration tab.

Configuring 802.1X with Guest VLANs



Note Supervisor Engine 6-E does *not* support this feature.

You can configure a guest VLAN for each 802.1X port on the Catalyst 4500 series switch to provide limited services to clients, such as downloading the 802.1X client. These clients might be upgrading their system for 802.1X authentication, and some hosts, such as Windows 98 systems, might not be 802.1X-capable.

When you enable a guest VLAN on an 802.1X port, the Catalyst 4500 series switch assigns clients to a guest VLAN provided (1) the authentication server does not receive a response to its EAPOL request or identity frame, or (2) the EAPOL packets are not sent by the client.

Starting with Cisco IOS Release 12.2(25)EWA, the Catalyst 4500 series switch maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, network access is denied. The EAPOL history is reset upon loss of the link.

Any number of 802.1X-incapable clients are allowed access when the switch port is moved to the guest VLAN. If an 802.1X-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on 802.1X ports in single-host or multiple-hosts mode.

**Note**

When a port is put into a guest VLAN, it is automatically placed into multihost mode, and an unlimited number of hosts can connect through the port. Changing the multihost configuration does not effect a port in a guest VLAN.

**Note**

Except for an RSPAN VLAN or a voice VLAN, you can configure any active VLAN as an 802.1X guest VLAN.

To configure 802.1X with guest VLAN on a port, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface <i>interface-id</i>	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 3	Switch(config-if)# switchport mode access or Switch(config-if)# switchport mode private-vlan host	Specifies a nontrunking, nontagged single VLAN Layer 2 interface. Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “ Default 802.1X Configuration ” section on page 37-22.
Step 5	Switch(config-if)# dot1x guest-vlan <i>vlan-id</i>	Enables a guest VLAN on a particular interface. To disable the guest VLAN feature on a particular port, use the no dot1x guest-vlan interface configuration command.
Step 6	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 7	Switch(config-if)# end	Returns to configuration mode.
Step 8	Switch(config)# end	Returns to privileged EXEC mode.

This example shows how to enable a regular VLAN 50 on Fast Ethernet 4/3 as a guest VLAN on a static access port:

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x guest-vlan 50
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

This example shows how to enable a secondary private VLAN 100 as a guest VLAN on a private VLAN host port:

```
Switch# configure terminal
Switch(config)# interface fa4/3
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x guest-vlan 100
Switch(config-if)# end
Switch#
```

To enable supplicants to be allowed into guest VLAN on a switch, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch# dot1x guest-vlan supplicant	(Optional) Enables supplicants to be allowed into the guest VLANs globally on the switch. Note Although not visible in the CLI for Cisco IOS Release 12.3(31)SG, legacy configurations that include the dot1x guest-vlan supplicant command still work. However, use of this command is not recommended because the authentication failed VLAN option obviates the need for this command. To disable the supplicant guest VLAN feature on a switch, use the no dot1x guest-vlan supplicant global configuration command.
Step 3	Switch(config)# interface interface-id	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 4	Switch(config-if)# switchport mode access or Switch(config-if)# switchport mode private-vlan host	Specifies a nontrunking, nontagged single VLAN Layer 2 interface. Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.
Step 5	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “ Default 802.1X Configuration ” section on page 37-22.
Step 6	Switch(config-if)# dot1x guest-vlan vlan-id	Specifies an active VLAN as an 802.1X guest VLAN. The range is 1 to 4094.
Step 7	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 8	Switch(config-if)# end	Returns to privileged EXEC mode.

	Command	Purpose
Step 9	Switch# show dot1x interface interface-id	Verifies your entries.
Step 10	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to enable the guest VLAN feature and to specify VLAN 5 as a guest VLAN:

```
Switch# configure terminal
Switch(config)# dot1x guest-vlan supplicant
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x guest-vlan 5
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Configuring 802.1X with MAC Authentication Bypass

To enable MAB, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface interface-id	Specifies the port to be configured, and enters interface configuration mode.
Step 3	Switch(config-if)# switchport mode access or Switch(config-if)# switchport mode private-vlan host	Specifies a nontrunking, nontagged single VLAN Layer 2 interface. Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “Default 802.1X Configuration” section on page 37-22.
Step 5	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 6	Switch(config-if)# dot1x mac-auth-bypass [eap]	Enables MAB on a switch.
Step 7	Switch(config)# end	Returns to privileged EXEC mode.
Step 8	Switch# show dot1x interface interface-id details	(Optional) Verifies your entries.
Step 9	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.



Note

Removing a 802.1X MAB configuration from a port does not impact the authorized/authenticated state of the port. If the port is in an unauthenticated state, it remains in that state. If the port is in an authenticated state because of MAB, the switch reverts to the 802.1X Authenticator. If the port was

already authorized with a MAC address and the MAB configuration was removed, the port remains in an authorized state until re-authentication occurs. At that time, if an 802.1X supplicant is detected on the wire, the MAC address is removed.

This example shows how to enable MAB on Gigabit Ethernet interface 3/3 and to verify the configuration:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x mac-auth-bypass
Switch(config-if)# end
Switch# show dot1x int g3/3 details
Dot1x Info for GigabitEthernet3/3
-----
PAE                               = AUTHENTICATOR
PortControl                        = AUTO
ControlDirection                  = Both
HostMode                           = SINGLE_HOST
ReAuthentication                   = Disabled
QuietPeriod                        = 60
ServerTimeout                      = 30
SuppTimeout                        = 30
ReAuthPeriod                       = 3600 (Locally configured)
ReAuthMax                          = 2
MaxReq                             = 2
TxPeriod                           = 1
RateLimitPeriod                   = 0
Mac-Auth-Bypass                   = Enabled

Dot1x Authenticator Client List
-----
Supplicant                         = 0000.0000.0001
  Auth SM State                    = AUTHENTICATED
  Auth BEND SM Stat = IDLE
Port Status                         = AUTHORIZED
Authentication Method              = MAB
Authorized By                       = Authentication Server
Vlan Policy                         = N/A

Switch#
```

Configuring 802.1X with Inaccessible Authentication Bypass



Note

Supervisor Engine 6-E does *not* support this feature.



Caution

You must configure the switch to monitor the state of the RADIUS server as described in the section [Configuring Switch-to-RADIUS-Server Communication, page 37-26](#) for Inaccessible Authentication Bypass to work properly. Specifically, you must configure the RADIUS test username, idle-time, deadtime and dead-criteria. Failure to do so results in the switch failing to detect that the RADIUS server has gone down, or prematurely marking a dead RADIUS server as alive again.

To configure a port as a critical port and to enable the Inaccessible Authentication Bypass feature, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# dot1x critical eapol	(Optional) Configures whether to send an EAPOL-Success packet when a port is critically-authorized partway through an EAP exchange. Note Some supplicants require this. The default is not to send EAPOL-Success packets when ports are critically-authorized.
Step 3	Switch(config)# dot1x critical recovery delay msec	(Optional) Specifies a throttle rate for the reinitialization of critically-authorized ports when the RADIUS server becomes available. The default throttle rate is 100 milliseconds. This means that 10 ports reinitialize per second.
Step 4	Switch(config)# interface interface-id	Specifies the port to be configured, and enters interface configuration mode.
Step 5	Switch(config-if)# switchport mode access or Switch(config-if)# switchport mode private-vlan host	Specifies a nontrunking, nontagged single VLAN Layer 2 interface. Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.
Step 6	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “Default 802.1X Configuration” section on page 37-22.
Step 7	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 8	Switch(config-if)# dot1x critical	Enables the Inaccessible Authentication Bypass feature on the port. To disable the feature, use the no dot1x critical interface configuration command.
Step 9	Switch(config-if)# dot1x critical vlan vlan	(Optional) Specifies a VLAN into which the port is assigned when it is critically authorized. Note Supervisor Engine 6-E does not support this feature. The default is to use the configured VLAN on the port.
Step 10	Switch(config-if)# dot1x critical recovery action reinitialize	(Optional) Specifies that the port should be reinitialized if it is critically authorized and RADIUS becomes available. The default is not to reinitialize the port.
Step 11	Switch(config)# end	Return to privileged EXEC mode.
Step 12	Switch# show dot1x interface interface-id details	(Optional) Verify your entries.
Step 13	Switch# copy running-config startup-config	(Optional) Save your entries in the configuration file.

The following example shows a full configuration of 802.1X with Inaccessible Authentication Bypass, including required AAA and RADIUS configuration as specified in the [“Enabling 802.1X Authentication”](#) section on page 37-23 and [“Configuring Switch-to-RADIUS-Server Communication”](#) section on page 37-26.

The RADIUS server configured is at IP address 10.1.2.3, using port 1812 for authentication and 1813 for accounting. The RADIUS secret key is *mykey*. The username used for the test server probes is *randomuser*. The test probes for both living and dead servers are generated once per minute. The interface FastEthernet 3/1 is configured to critically authenticate into VLAN 17 when AAA becomes unresponsive, and to reinitialize automatically when AAA becomes available again.

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# radius-server host 10.1.2.3 auth-port 1812 acct-port 1813 test username
randomuser idle-time 1 key mykey
Switch(config)# radius deadtime 1
Switch(config)# radius dead-criteria time 15 tries 3
Switch(config)# interface f3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x critical
Switch(config-if)# dot1x critical vlan 17
Switch(config-if)# dot1x critical recovery action reinitialize
Switch(config-if)# end
Switch# show dot1x int fastethernet 3/1 det
```

```
Dot1x Info for FastEthernet3/1
-----
PAE = AUTHENTICATOR
PortControl = AUTO
ControlDirection = Both
HostMode = SINGLE_HOST
ReAuthentication = Disabled
QuietPeriod = 60
ServerTimeout = 30
SuppTimeout = 30
ReAuthPeriod = 3600 (Locally configured)
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
RateLimitPeriod = 0
Critical-Auth = Enabled
Critical Recovery Action = Reinitialize
Critical-Auth VLAN = 17
```

```
Dot1x Authenticator Client List
-----
Supplicant = 0000.0000.0001
```

```
Auth SM State = AUTHENTICATING
Auth BEND SM Stat = RESPONSE
Port Status = AUTHORIZED
Authentication Method = Dot1x
Authorized By = Critical-Auth
Operational HostMode = SINGLE_HOST
Vlan Policy = 17
```

```
Switch#
```

Configuring 802.1X with Unidirectional Controlled Port



Note Supervisor Engine 6-E does *not* support this feature.

To configure unidirectional controlled port, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface <i>interface-id</i>	Specifies the port to be configured, and enter interface configuration mode.
Step 3	Switch(config-if)# switchport mode access or Switch(config-if)# switchport mode private-vlan host	Specifies a nontrunking, nontagged single VLAN Layer 2 interface. Specifies that the ports with a valid PVLAN trunk association become active host private VLAN trunk ports.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “Default 802.1X Configuration” section on page 37-22.
Step 5	Switch(config-if)# dot1x control-direction {in both}	Enables unidirectional port control on a per-port basis.
Step 6	Switch(config)# end	Returns to privileged EXEC mode.
Step 7	Switch# show dot1x interface <i>interface-id</i> details	(Optional) Verifies your entries.
Step 8	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.



Note Unidirectional Controlled Port only works when Spanning Tree Portfast is enabled on the port.

When a device is enabled for unidirectional controlled port (also termed Wake On LAN), its interface stays up when the device sleeps. So, the port connected to the device displays as link up (connected). When you forward special packets to the port, the device wakes up.

This example shows how to enable unidirectional port control:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/3
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x control-direction in
Switch(config-if)# end
Switch# show dot1x int g3/3
Dot1x Info for GigabitEthernet3/3
-----
PAE                               = AUTHENTICATOR
PortControl                       = AUTO
ControlDirection                 = In (Inactive)
HostMode                         = SINGLE_HOST
ReAuthentication                 = Disabled
QuietPeriod                      = 60
ServerTimeout                    = 30
SuppTimeout                      = 30
```

```

ReAuthPeriod          = 3600 (Locally configured)
ReAuthMax             = 2
MaxReq                = 2
TxPeriod              = 30
RateLimitPeriod       = 0

Switch#

```

Configuring 802.1X with Authentication Failed VLAN Assignment



Note Supervisor Engine 6-E does *not* support this feature.

By configuring authentication-failed VLAN alignment on any Layer 2 port on the Catalyst 4500 series switch, you can provide limited network services to clients that fail the authentication process.



Note You can use authentication-failed VLAN assignment with other security features, such as Dynamic ARP Inspection (DAI), Dynamic Host Configuration Protocol (DHCP) snooping, and IP Source Guard. Each of these features can be enabled and disabled independently on the authentication-failed VLAN.

To configure 802.1X with authentication-failed VLAN assignment, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface <i>interface-id</i>	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 3	Switch(config-if)# switchport mode access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 5	Switch(config-if)# dot1x auth-fail vlan <i>vlan-id</i>	Enables authentication-failed VLAN on a particular interface. To disable the authentication-failed VLAN feature on a particular port, use the no dot1x auth-fail vlan interface configuration command.
Step 6	Switch(config-if)# dot1x auth-fail max-attempts <i>max-attempts</i>	Configure a maximum number of attempts before the port is moved to authentication-failed VLAN. Default is 3 attempts.
Step 7	Switch(config-if)# end	Returns to configuration mode.
Step 8	Switch(config)# end	Returns to privileged EXEC mode.
Step 9	Switch# show dot1x interface <i>interface-id</i> details	(Optional) Verifies your entries.
Step 10	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to enable a regular VLAN 40 on Fast Ethernet 4/3 as a authentication-failed VLAN on a static access port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet3/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x auth-fail vlan 40
Switch(config-if)# dot1x auth-fail max-attempts 5
Switch(config-if)# end
Switch(config)# end
Switch# show dot1x all
Dot1x Info for interface GigabitEthernet3/1
-----
PortStatus      = AUTHORIZED(AUTH-FAIL-VLAN)
MaxReq          = 2
MaxAuthReq      = 2
HostMode        = Single(AUTH-FAIL-VLAN)
PortControl     = Auto
QuietPeriod     = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod    = 3600 Seconds
ServerTimeout   = 30 Seconds
SuppTimeout     = 30 Seconds
TxPeriod        = 30 Seconds
Guest-Vlan      = 6
Switch
```

Configuring 802.1X with Voice VLAN



Note

You must configure 802.1X and voice VLAN at the same time.

To enable 802.1X with voice VLAN, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface <i>interface-id</i>	Enters interface configuration mode.
Step 3	Switch(config-if)# switchport access vlan <i>vlan-id</i>	Sets the VLAN for a switched interface in access mode.
Step 4	Switch(config-if)# switchport mode access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 5	Switch(config-if)# switchport voice vlan <i>vlan-id</i>	Sets the voice VLAN for the interface.
Step 6	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “ Default 802.1X Configuration ” section on page 37-22.
Step 7	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 8	Switch(config-if)# end	Returns to configuration mode.
Step 9	Switch(config)# end	Returns to privileged EXEC mode.

	Command	Purpose
Step 10	Switch# show dot1x interface interface-id details	(Optional) Verifies your entries.
Step 11	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to enable 802.1X with voice VLAN feature on Fast Ethernet interface 5/9:

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport access vlan 2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 10
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch(config)# end
Switch#
```

Enabling Periodic Reauthentication

You can enable periodic 802.1X client reauthentication and specify how often it occurs. If you do not specify a time value before enabling reauthentication, the interval between reauthentication attempts is 3600 seconds.

Automatic 802.1X client reauthentication is a per-interface setting and can be set for clients connected to individual ports. To manually reauthenticate the client connected to a specific port, see the [“Changing the Quiet Period”](#) section on page 37-44.

To enable periodic reauthentication of the client and to configure the number of seconds between reauthentication attempts, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface interface-id	Enters interface configuration mode and specifies the interface to be enabled for periodic reauthentication.
Step 3	Switch(config-if)# switchport mode access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “Default 802.1X Configuration” section on page 37-22.
Step 5	Switch(config-if)# dot1x re-authentication	Enables periodic reauthentication of the client, which is disabled by default. To disable periodic reauthentication, use the no dot1x re-authentication interface configuration command.

	Command	Purpose
Step 6	Switch(config-if)# dot1x timeout reauth-period {seconds server}	Specifies the number of seconds between reauthentication attempts or have the switch use a RADIUS-provided session timeout. The range is 1 to 65,535; the default is 3600 seconds. To return to the default number of seconds between reauthentication attempts, use the no dot1x timeout reauth-period global configuration command. This command affects the behavior of the switch only if periodic reauthentication is enabled.
Step 7	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 8	Switch(config-if)# end	Returns to privileged EXEC mode.

This example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000:

```
Switch# configure terminal
Switch(config)# interface fastethernet5/9
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x re-authentication
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Enabling Multiple Hosts

You can attach multiple hosts (clients) to a single 802.1X-enabled port as shown in [Figure 37-7 on page 37-21](#). In this mode, when the port is authorized, all other hosts that are indirectly attached to the port are granted access to the network. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the switch denies access to the network for all wireless access point-attached clients.

To allow multiple hosts (clients) on an 802.1X-authorized port that has the **dot1x port-control** interface configuration command set to **auto**, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface interface-id	Enters interface configuration mode and specifies the interface to which multiple hosts are indirectly attached.
Step 3	Switch(config-if)# switchport mode access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “ Default 802.1X Configuration ” section on page 37-22.

	Command	Purpose
Step 5	Switch(config-if)# dot1x host-mode multiple-hosts	Allows multiple hosts (clients) on an 802.1X-authorized port. Note Ensure that the dot1x port-control interface configuration command set is set to auto for the specified interface. To disable multiple hosts on the port, use the no dot1x host-mode multiple-hosts interface configuration command.
Step 6	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 7	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 8	Switch# show dot1x all interface interface-id	Verifies your entries.
Step 9	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x host-mode multiple-hosts
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time, and then tries again. The idle time is determined by the **quiet-period** value. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering a number smaller than the default.

To change the quiet period, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface interface-id	Enters interface configuration mode and specifies the interface to be enabled for timeout quiet-period .
Step 3	Switch(config-if)# switchport mode access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “ Default 802.1X Configuration ” section on page 37-22.
Step 5	Switch(config-if)# dot1x timeout quiet-period seconds	Sets the number of seconds that the switch remains in the quiet-period following a failed authentication exchange with the client. To return to the default quiet-period, use the no dot1x timeout quiet-period configuration command. The range is 0 to 65,535 seconds; the default is 60.

	Command	Purpose
Step 6	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.
Step 7	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 8	Switch# show dot1x all	Verifies your entries.
Step 9	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to set the **quiet-period** on the switch to 30 seconds:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout quiet-period 30
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time) and then retransmits the frame.



Note

You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To change the amount of time that the switch waits for client notification, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface interface-id	Enters interface configuration mode and specifies the interface to be enabled for timeout tx-period.
Step 3	Switch(config-if)# switchport mode access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “Default 802.1X Configuration” section on page 37-22 .
Step 5	Switch(config-if)# dot1x timeout tx-period seconds	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65,535 seconds; the default is 30. To return to the default retransmission time, use the no dot1x timeout tx-period interface configuration command.
Step 6	Switch(config-if)# dot1x port-control auto	Enables 802.1X authentication on the interface.

	Command	Purpose
Step 7	Switch(config-if)# end	Returns to privileged EXEC mode.
Step 8	Switch# show dot1x all	Verifies your entries.
Step 9	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

This example shows how to set the retransmission time to 60 seconds:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission times, you can change the number of times that the switch sends EAP-Request/Identity and other EAP-Request frames to the client before restarting the authentication process. The number of EAP-Request/Identity retransmissions is controlled by the **dot1x max-reauth-req** command; the number of retransmissions for other EAP-Request frames is controlled by the **dot1x max-req** command.



Note

You should change the default values of these commands only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

To set the switch-to-client frame-retransmission numbers, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# interface interface-id	Enters interface configuration mode and specifies the interface to be enabled for max-reauth-req and/or max-req .
Step 3	Switch(config-if)# switchport mode access	Specifies a non-trunking, nontagged single VLAN Layer 2 interface.
Step 4	Switch(config-if)# dot1x pae authenticator	Enables 802.1X authentication on the port with default parameters. Refer to the “Default 802.1X Configuration” section on page 37-22.

	Command	Purpose
Step 5	<pre>Switch(config-if)# dot1x max-req count or Switch(config-if)# dot1x max-reauth-req count</pre>	<p>Specifies the number of times EAPOL DATA packets are re-transmitted (if lost, or not replied to). For example, if you have a supplicant in the midst of authenticating and it experiences a problem, the authenticator will re-transmit requests for data 3 times before giving up on the authentication request. The range for <i>count</i> is 1 to 10; the default is 2.</p> <p>Specifies the timer for EAPOL-Identity-Request frames (only). If you plug in a device incapable of 802.1X, 3 EAPOL-Id-Req frames will go out on the wire before the state machine resets. Alternatively, if you have configured Guest-VLAN, 3 frames will go out on the wire before the port is enabled. This parameter has a default value of 2.</p> <p>To return to the default retransmission number, use the no dot1x max-req and no dot1x max-reauth-req global configuration command.</p>
Step 6	<pre>Switch(config-if)# dot1x port-control auto</pre>	Enables 802.1X authentication on the interface.
Step 7	<pre>Switch(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 8	<pre>Switch# show dot1x all</pre>	Verifies your entries.
Step 9	<pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

This example shows how to set 5 as the number of times that the switch retransmits an EAP-request/identity request before restarting the authentication process:

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x max-reauth-req 5
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
Switch#
```

Manually Reauthenticating a Client Connected to a Port

You can manually reauthenticate a client connected to a specific port at any time by entering the **dot1x re-authenticate interface** privileged EXEC command. If you want to enable or disable periodic reauthentication, see the [“Enabling Periodic Reauthentication”](#) section on page 37-42.

This example shows how to manually reauthenticate the client connected to Fast Ethernet port 1/1:

```
Switch# dot1x re-authenticate interface fastethernet1/1
Starting reauthentication on FastEthernet1/1
```

Initializing the 802.1X Authentication State

The **dot1x initialize** command causes the authentication process to be restarted irrespective of the state it is in currently.

This example shows how to restart the authentication process on Fast Ethernet port 1/1:

```
Switch# dot1x initialize interface fastethernet1/1
```

This example shows how to restart the authentication process on all ports of the switch:

```
Switch# dot1x initialize
```

Removing 802.1X Client Information

The **clear dot1x** command causes all existing supplicants to be completely deleted from an interface or from all the interfaces on a switch.

This example shows how to remove 802.1X client information on Fast Ethernet port 1/1:

```
Switch# clear dot1x interface fastethernet1/1
```

This example shows how to remove 802.1X client information on all ports of the switch:

```
Switch# clear dot1x all
```

Resetting the 802.1X Configuration to the Default Values

To reset the 802.1X configuration to the default values, perform this task:

	Command	Purpose
Step 1	Switch# configure terminal	Enters global configuration mode.
Step 2	Switch(config)# dot1x default	Resets the configurable 802.1X parameters to the default values.
Step 3	Switch(config)# end	Returns to privileged EXEC mode.
Step 4	Switch# show dot1x all	Verifies your entries.
Step 5	Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Displaying 802.1X Statistics and Status

To display 802.1X statistics for all interfaces, use the **show dot1x all statistics** privileged EXEC command.

To display the 802.1X administrative and operational status for the switch, use the **show dot1x all details** privileged EXEC command. To display the 802.1X administrative and operational status for a specific interface, use the **show dot1x interface details** privileged EXEC command.