



## Configuring 802.1x Port-Based Authentication

This chapter describes how to configure IEEE 802.1x port-based authentication on the Catalyst 2950 or Catalyst 2955 switch to prevent unauthorized devices (clients) from gaining access to the network.



### Note

For complete syntax and usage information for the commands used in this chapter, refer to the command reference for this release.

This chapter consists of these sections:

- [Understanding 802.1x Port-Based Authentication, page 10-1](#)
- [Configuring 802.1x Authentication, page 10-9](#)
- [Displaying 802.1x Statistics and Status, page 10-21](#)

## Understanding 802.1x Port-Based Authentication

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports unless they are properly authenticated. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

These sections describe 802.1x port-based authentication:

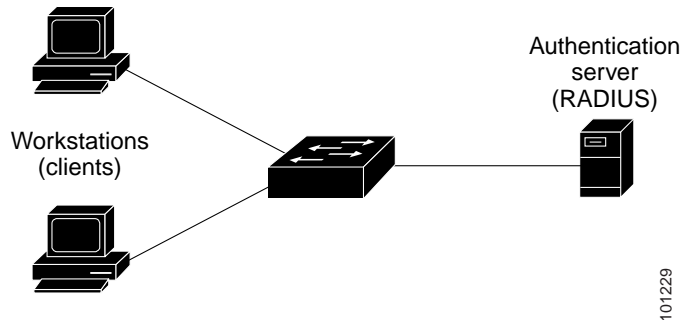
- [Device Roles, page 10-2](#)
- [Authentication Initiation and Message Exchange, page 10-3](#)
- [Ports in Authorized and Unauthorized States, page 10-4](#)
- [802.1x Accounting, page 10-5](#)
- [Supported Topologies, page 10-5](#)
- [Using 802.1x with Port Security, page 10-6](#)
- [Using 802.1x with Voice VLAN Ports, page 10-7](#)

- [Using 802.1x with VLAN Assignment, page 10-7](#)
- [Using 802.1x with Guest VLAN, page 10-8](#)

## Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles as shown in [Figure 10-1](#).

**Figure 10-1 802.1x Device Roles**



- *Client*—the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the *supplicant* in the IEEE 802.1x specification.)



### Note

To resolve Windows XP network connectivity and 802.1x authentication issues, read the Microsoft Knowledge Base article at this URL:  
<http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP>

- *Authentication server*—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the RADIUS security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server. It is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- *Switch* (edge switch or wireless access point)—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) 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 includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the 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 re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must

support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

The devices that can act as intermediaries include the Catalyst 3750, Catalyst 3550, Catalyst 2970, Catalyst 2955, Catalyst 2950, Catalyst 2940 switches, or a wireless access point. These devices must be running software that supports the RADIUS client and 802.1x.

## Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. 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.



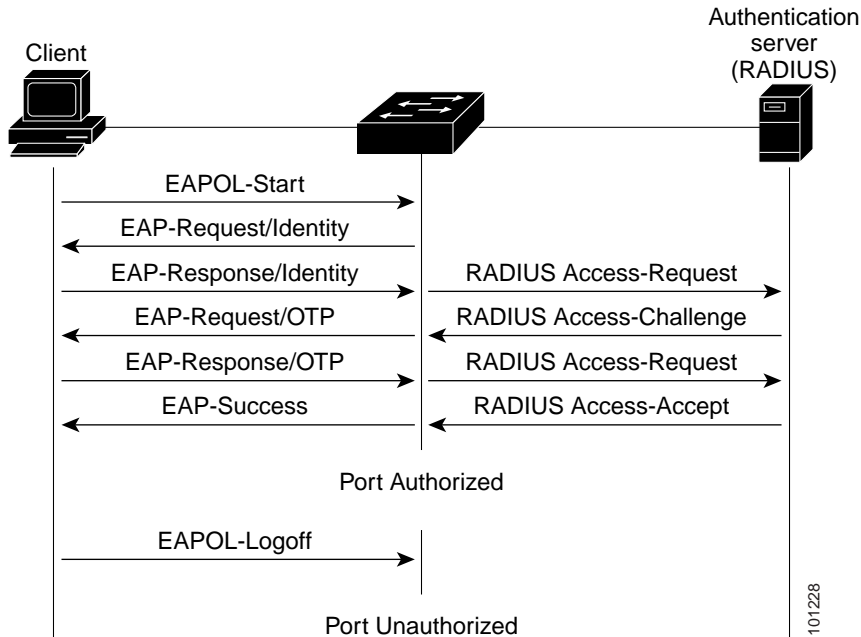
### Note

If 802.1x is not enabled or supported on the network access device, 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 sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated. For more information, see the [“Ports in Authorized and Unauthorized States” section on page 10-4](#).

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. For more information, see the [“Ports in Authorized and Unauthorized States” section on page 10-4](#).

The specific exchange of EAP frames depends on the authentication method being used. [Figure 10-2](#) shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 10-2 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 client that does not support 802.1x 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.

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

You control the port authorization state by using 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 any authentication exchange required. The port sends and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
- **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. Each client attempting to access the network is uniquely identified by the switch by using 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 the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

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

## 802.1x Accounting

The IEEE 802.1x standard defines how users are authorized and authenticated for network access but does not keep track of network usage. 802.1x accounting is disabled by default. You can enable 802.1x accounting to monitor this activity on 802.1x-enabled ports:

- User successfully authenticates.
- User logs off.
- Link-down occurs.
- Re-authentication successfully occurs.
- Re-authentication fails.

The switch does not log 802.1x accounting information. Instead, it sends this information to the RADIUS server, which must be configured to log accounting messages.

## Supported Topologies

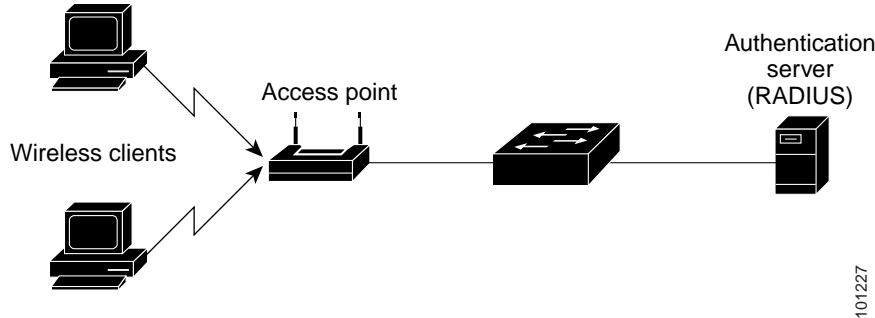
The 802.1x port-based authentication is supported in two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration (see [Figure 10-1 on page 10-2](#)), only one client can be connected to the 802.1x-enabled switch port. 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.

[Figure 10-3](#) shows 802.1x port-based authentication in a wireless LAN. The 802.1x port is configured as a multiple-hosts port that becomes authorized as soon as one client is authenticated. When the port is authorized, all other hosts indirectly attached to the port are granted access to the network. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), the switch denies access to the network to all of the attached clients. In this topology, the wireless access point is responsible for authenticating the clients attached to it, and the wireless access point acts as a client to the switch.

Figure 10-3 Wireless LAN Example



## Using 802.1x with Port Security

For switches running the enhanced software image (EI), you can enable an 802.1x port for port security in either single-host or multiple-hosts mode. (You must also configure port security on the port by using the **switchport port-security** interface configuration command.) When you enable port security and 802.1x on a port, 802.1x authenticates the port, and port security manages network access for all MAC addresses, including that of the client. You can then limit the number or group of clients that can access the network through an 802.1x port.

These are some examples of the interaction between 802.1x and port security on the 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 the client is authenticated, but port security table is full. This can happen if the maximum number of secure hosts has been statically configured, or if the client ages out of the secure host table. If the client's address is aged out, its place in the secure host table can be taken by another host.
- The port security violation modes determine the action for security violations. For more information, see the [“Security Violations” section on page 22-8](#).
- 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 takes place.
- If the port is administratively shut down, the port becomes unauthenticated, and all dynamic entries are removed from the secure host table.
- Port security and a voice VLAN can be configured simultaneously on an 802.1x port that is in either single-host or multiple-hosts mode. Port security applies to both the voice VLAN identifier (VVID) and the port VLAN identifier (PVID).
- When an 802.1x client address is manually removed from the port security table, we recommend that you re-authenticate the client by entering the **dot1x re-authenticate** privileged EXEC command.

For more information about enabling port security on your switch, see the [“Configuring Port Security” section on page 22-7](#).

## Using 802.1x with Voice VLAN Ports

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

- VVID to carry voice traffic to and from the IP phone. The VVID is used to configure the IP phone connected to the port.
- 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 PVID and a VVID. This configuration allows voice traffic and data traffic to be separated onto different VLANs.

When you enable the single-host mode, only one 802.1x client is allowed on the primary VLAN; other workstations are blocked. When you enable the multiple-hosts mode and an 802.1x client is authenticated on the primary VLAN, additional clients on the voice VLAN are unrestricted after 802.1x authentication succeeds on the primary VLAN.

A voice VLAN port becomes active when there is link, and the device MAC address appears after the first CDP message from the IP phone. 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 port VLAN that is equal to a voice VLAN.

For more information about voice VLANs, see [Chapter 19, “Configuring Voice VLAN.”](#)

## Using 802.1x with VLAN Assignment

For switches running the EI, you can limit network access for certain users by using VLAN assignment. After successful 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. The RADIUS server database maintains the username-to-VLAN mappings, which assigns the VLAN based on the username of the client connected to the switch port.

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 or if 802.1x authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1x authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error.  
Configuration errors could include a VLAN specified for a routed port, a malformed VLAN ID, a nonexistent or internal (routed port) VLAN ID, or attempted assignment to a voice VLAN ID.
- If 802.1x authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If the multiple-hosts mode is enabled on an 802.1x port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- If port security is enabled on an 802.1x port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If 802.1x is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is placed in the configured access VLAN.

- If an 802.1x port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1x with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).

To configure VLAN assignment you need to perform these tasks:

- Enable AAA authorization.
- 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. The RADIUS server must return these attributes to the switch:
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

Attribute [64] must contain the value *VLAN* (type 13). Attribute [65] must contain the value *802* (type 6). Attribute [81] specifies the *VLAN name* or *VLAN ID* assigned to the 802.1x-authenticated user.

For examples of tunnel attributes, see the [“Configuring the Switch to Use Vendor-Specific RADIUS Attributes”](#) section on page 9-29.

## Using 802.1x with Guest VLAN

For switches running the EI, you can configure a guest VLAN for each 802.1x port on the switch to provide limited services to clients (for example, how to download 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.

If an 802.1x port is configured, the switch assigns clients to a guest VLAN for the 802.1x port when one of these situations occurs:

- The authentication server does not receive a response to its EAPOL request/identity frame.
- 802.1x EAPOL packets are not sent by the client.
- New 802.1x EAPOL packets are sent by the client, but authentication fails.

Any number of hosts are allowed access when the switch port is moved to the guest VLAN. If an 802.1x-capable host 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.

Any number of hosts are allowed access once the switch port is moved to the guest VLAN. If an 802.1x-capable host 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 and multiple-hosts modes.

You can configure any VLAN, except RSPAN VLANs or voice VLAN IDs (VVIDs), as an 802.1x guest VLAN. The guest VLAN feature is not supported on trunk ports; it is supported only on access ports.

For configuration steps, see the [“Configuring a Guest VLAN”](#) section on page 10-18.

# Configuring 802.1x Authentication

These sections describe how to configure 802.1x port-based authentication on your switch:

- [Default 802.1x Configuration, page 10-9](#)
- [802.1x Configuration Guidelines, page 10-10](#)
- [Upgrading from a Previous Software Release, page 10-11](#)
- [Enabling 802.1x Authentication, page 10-11](#) (required)
- [Configuring the Switch-to-RADIUS-Server Communication, page 10-13](#) (required)
- [Enabling Periodic Re-Authentication, page 10-14](#) (optional)
- [Manually Re-Authenticating a Client Connected to a Port, page 10-15](#) (optional)
- [Changing the Quiet Period, page 10-15](#) (optional)
- [Changing the Switch-to-Client Retransmission Time, page 10-15](#) (optional)
- [Setting the Switch-to-Client Frame-Retransmission Number, page 10-16](#) (optional)
- [Configuring the Host Mode, page 10-17](#) (optional)
- [Configuring a Guest VLAN, page 10-18](#) (optional)
- [Resetting the 802.1x Configuration to the Default Values, page 10-18](#) (optional)
- [Configuring 802.1x Authentication, page 10-19](#) (optional)
- [Configuring 802.1x Accounting, page 10-20](#) (optional)

## Default 802.1x Configuration

[Table 10-1](#) shows the default 802.1x configuration.

**Table 10-1** *Default 802.1x Configuration*

Feature	Default Setting
AAA	Disabled.
RADIUS server <ul style="list-style-type: none"> <li>• IP address</li> <li>• UDP authentication port</li> <li>• Key</li> </ul>	<ul style="list-style-type: none"> <li>• None specified.</li> <li>• 1812.</li> <li>• None specified.</li> </ul>
Switch 802.1x enable state	Disabled.
Per-interface 802.1x enable state	Disabled (force-authorized). The port sends and receives normal traffic without 802.1x-based authentication of the client.
Periodic re-authentication	Disabled.
Number of seconds between re-authentication attempts	3600 seconds.

*Table 10-1 Default 802.1x Configuration (continued)*

Feature	Default Setting
Quiet period	60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).
Retransmission time	30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before resending the request).
Maximum retransmission number	2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).
Host mode	Single-host mode.
Guest VLAN	None specified.
Client timeout period	30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before resending the request to the client).
Authentication server timeout period	30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before resending the response to the server. This setting is not configurable.)

## 802.1x Configuration Guidelines

These are the 802.1x authentication configuration guidelines:

- When 802.1x is enabled, ports are authenticated before any other Layer 2 features are enabled.
- The 802.1x protocol is supported on Layer 2 static-access ports and voice VLAN ports, but it is not supported on these port types:
  - Trunk port—If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.
  - Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1x on a dynamic port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to dynamic, the port mode is not changed.
  - Dynamic-access ports—If you try to enable 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1x is not enabled. If you try to change an 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
  - EtherChannel ports—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x on an EtherChannel port, an error message appears, and 802.1x is not enabled.

- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1x on a port that is a SPAN destination, an RSPAN destination, or an RSPAN reflector port. However, 802.1x is disabled until the port is removed as a SPAN destination, an RSPAN destination, or an RSPAN reflector port. You can enable 802.1x on a SPAN or RSPAN source port.
- LRE switch ports—802.1x is not supported on an LRE switch interface that is connected to a Cisco 585 LRE CPE device.
- You can configure any VLAN, except RSPAN VLANs or voice VVIDs, as an 802.1x guest VLAN. The guest VLAN feature is not supported trunk ports; it is supported only on access ports.
- When 802.1x is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- The 802.1x with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VMPS.
- Before globally enabling 802.1x on a switch by entering the **dot1x system-auth-control** global configuration command, remove the EtherChannel configuration from the interfaces on which 802.1x and EtherChannel are configured.
- If you are using a device running the Cisco Access Control Server (ACS) application for 802.1x authentication with EAP-Transparent LAN Services (TLS) and EAP-MD5 and your switch is running Cisco IOS Release 12.1(14)EA1, make sure that the device is running ACS Version 3.2.1 or later.
- After you configure a guest VLAN for an 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can also change the settings for restarting the 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the 802.1x authentication process (802.1x quiet period and switch-to-client transmission time).

## Upgrading from a Previous Software Release

In Cisco IOS Release 12.1(14)EA1, the implementation for 802.1x changed from the previous release. Some global configuration commands became interface configuration commands, and new commands were added.

If you have 802.1x configured on the switch and you upgrade to Cisco IOS Release 12.1(14)EA1 or later, the configuration file will not contain the new commands, and 802.1x will not operate. After the upgrade is complete, make sure to globally enable 802.1x by using the **dot1x system-auth-control** global configuration command. If 802.1x was running in multiple-hosts mode on an interface in the previous release, make sure to reconfigure it by using the **dot1x host-mode multi-host** interface configuration command.

## Enabling 802.1x Authentication

To enable 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method 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.

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

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication. This procedure is required.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>aaa new-model</b>	Enable AAA.
Step 3	<b>aaa authentication dot1x {default} method1 [method2...]</b>	<p>Create an 802.1x authentication method list.</p> <p>To create a default list that is used when a named list is <i>not</i> specified in the <b>authentication</b> command, use the <b>default</b> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces.</p> <p>Enter at least one of these keywords:</p> <ul style="list-style-type: none"> <li>• <b>group radius</b>—Use the list of all RADIUS servers for authentication.</li> <li>• <b>none</b>—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.</li> </ul>
Step 4	<b>dot1x system-auth-control</b>	Enable 802.1x authentication globally on the switch.
Step 5	<b>aaa authorization network {default} group radius</b>	(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as VLAN assignment.
Step 6	<b>interface interface-id</b>	Specify the interface connected to the client to be enabled for 802.1x authentication, and enter interface configuration mode.
Step 7	<b>dot1x port-control auto</b>	<p>Enable 802.1x authentication on the interface.</p> <p>For feature interaction information, see the “<a href="#">802.1x Configuration Guidelines</a>” section on page 10-10.</p>
Step 8	<b>end</b>	Return to privileged EXEC mode.
Step 9	<b>show dot1x</b>	<p>Verify your entries.</p> <p>Check the Status column in the 802.1x Port Summary section of the display. An <i>enabled</i> status means the port-control value is set either to <b>auto</b> or to <b>force-unauthorized</b>.</p>
Step 10	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable 802.1x AAA authentication, use the **no aaa authentication dot1x {default | list-name}** global configuration command. To disable 802.1x AAA authorization, use the **no aaa authorization** global configuration command. To disable 802.1x authentication on the switch, use the **no dot1x system-auth-control** global configuration command.

This example shows how to enable AAA and 802.1x on a port:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

## Configuring the Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, 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 that they were configured.

Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>radius-server host</b> { <i>hostname</i>   <i>ip-address</i> } <b>auth-port</b> <i>port-number</i> <b>key</b> <i>string</i>	<p>Configure the RADIUS server parameters on the switch.</p> <p>For <i>hostname</i>   <i>ip-address</i>, specify the host name or IP address of the remote RADIUS server.</p> <p>For <b>auth-port</b> <i>port-number</i>, specify the UDP destination port for authentication requests. The default is 1812.</p> <p>For <b>key</b> <i>string</i>, specify 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><b>Note</b> Always configure the key as the last item in the <b>radius-server host</b> 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, re-enter this command.</p>
Step 3	<b>end</b>	Return to privileged EXEC mode.
Step 4	<b>show running-config</b>	Verify your entries.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To delete the specified RADIUS server, use the **no radius-server host** {*hostname* | *ip-address*} global configuration command.

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server, to use port 1612 as the authorization port, and to set the encryption key to *rad123*, matching the key on the RADIUS server:

```
Switch(config)# radius-server host 172.120.39.46 auth-port 1612 key rad123
```

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. For more information, see the “[Configuring Settings for All RADIUS Servers](#)” section on page 9-29.

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. For more information, refer to the RADIUS server documentation.

## Enabling Periodic Re-Authentication

You can enable periodic 802.1x client re-authentication and specify how often it occurs. If you do not specify a time period before enabling re-authentication, the number of seconds between re-authentication attempts is 3600.

Beginning in privileged EXEC mode, follow these steps to enable periodic re-authentication of the client and to configure the number of seconds between re-authentication attempts. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>dot1x reauthentication</b>	Enable periodic re-authentication of the client, which is disabled by default.
Step 4	<b>dot1x timeout reauth-period</b> <i>seconds</i>	Set the number of seconds between re-authentication attempts. The range is 1 to 65535; the default is 3600 seconds. This command affects the behavior of the switch only if periodic re-authentication is enabled.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show dot1x interface</b> <i>interface-id</i>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable periodic re-authentication, use the **no dot1x reauthentication** interface configuration command. To return to the default number of seconds between re-authentication attempts, use the **no dot1x timeout reauth-period** global configuration command.

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

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

## Manually Re-Authenticating a Client Connected to a Port

You can manually re-authenticate the client connected to a specific port at any time by entering the **dot1x re-authenticate interface *interface-id*** privileged EXEC command. This step is optional. If you want to enable or disable periodic re-authentication, see the “[Enabling Periodic Re-Authentication](#)” section on page 10-14.

This example shows how to manually re-authenticate the client connected to a port:

```
Switch# dot1x re-authenticate interface fastethernet0/1
```

## 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 smaller number than the default.

Beginning in privileged EXEC mode, follow these steps to change the quiet period. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>dot1x timeout quiet-period <i>seconds</i></b>	Set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show dot1x interface <i>interface-id</i></b>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default quiet time, use the **no dot1x timeout quiet-period** interface configuration command.

This example shows how to set the quiet time on the switch to 30 seconds:

```
Switch(config-if)# dot1x timeout quiet-period 30
```

## 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 resends 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.

Beginning in privileged EXEC mode, follow these steps to change the amount of time that the switch waits for client notification. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>dot1x timeout tx-period</b> <i>seconds</i>	Set the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. The range is 1 to 65535 seconds; the default is 30.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show dot1x interface</b> <i>interface-id</i>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default retransmission time, use the **no dot1x timeout tx-period** interface configuration command.

This example shows how to set 60 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request:

```
Switch(config-if)# dot1x timeout tx-period 60
```

## Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.



### 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.

Beginning in privileged EXEC mode, follow these steps to set the switch-to-client frame-retransmission number. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	<b>dot1x max-req</b> <i>count</i>	Set the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show dot1x interface</b> <i>interface-id</i>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To return to the default retransmission number, use the **no dot1x max-req** interface configuration command.

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

```
Switch(config-if)# dot1x max-req 5
```

## Configuring the Host Mode

You can configure an 802.1x port for single-host or for multiple-hosts mode. In single-host mode, only one host is allowed on an 802.1x port. When the host is authenticated, the port is placed in the authorized state. When the host leaves the port, the port becomes unauthorized. Packets from hosts other than the authenticated one are dropped.

You can attach multiple hosts to a single 802.1x-enabled port as shown in [Figure 10-3 on page 10-6](#). In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), all attached clients are denied access to the network.

With the multiple-hosts mode enabled, you can use 802.1x to authenticate the port and port security to manage network access for all MAC addresses, including that of the client (for switches running the EI).

Beginning in privileged EXEC mode, follow these steps to allow multiple hosts (clients) on an 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to which multiple hosts are indirectly attached, and enter interface configuration mode.
Step 3	<b>dot1x host-mode multi-host</b>	Allow multiple hosts (clients) on an 802.1x-authorized port. Make sure that the <b>dot1x port-control</b> interface configuration command set is set to <b>auto</b> for the specified interface.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show dot1x interface</b> <i>interface-id</i>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable multiple hosts on the port, use the **no dot1x host-mode multi-host** interface configuration command.

This example shows how to enable a port to allow multiple hosts:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

## Configuring a Guest VLAN

For switches running the EI, when you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its EAPOL request/identity frame. Clients that are 802.1x-capable but fail authentication are not granted access to the network. The switch supports guest VLANs in single-host or multiple-hosts mode.

Beginning in privileged EXEC mode, follow these steps to configure a guest VLAN. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode. For the supported interface types, see the “ <a href="#">802.1x Configuration Guidelines</a> ” section on page 10-10.
Step 3	<b>dot1x guest-vlan</b> <i>vlan-id</i>	Specify an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094.  Any VLAN can be configured as an 802.1x guest VLAN except RSPAN VLANs or voice VLANs.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show dot1x interface</b> <i>interface-id</i>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable and remove the guest VLAN, use the **no dot1x guest-vlan** interface configuration command. The port returns to the unauthorized state.

This example shows how to enable VLAN 9 as an 802.1x guest VLAN on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x guest-vlan 9
```

This example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request, and to enable VLAN 2 as an 802.1x guest VLAN when an 802.1x port is connected to a DHCP client:

```
Switch(config-if)# dot1x timeout quiet-period 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

## Resetting the 802.1x Configuration to the Default Values

Beginning in privileged EXEC mode, follow these steps to reset the 802.1x configuration to the default values.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.

	Command	Purpose
Step 3	<b>dot1x default</b>	Reset the configurable 802.1x parameters to the default values.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show dot1x interface</b> <i>interface-id</i>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## Configuring 802.1x Authentication

To configure 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users. If that method fails to respond, the software selects the next authentication method in the method 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.

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

This is the 802.1x authentication, authorization and accounting process:

- 
- Step 1 A user connects to a port on the switch.
  - Step 2 Authentication is performed.
  - Step 3 VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.
  - Step 4 The switch sends a start message to an accounting server.
  - Step 5 Re-authentication is performed, as necessary.
  - Step 6 The switch sends an interim accounting update to the accounting server that is based on the result of re-authentication.
  - Step 7 The user disconnects from the port.
  - Step 8 The switch sends a stop message to the accounting server.
- 

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>aaa new-model</b>	Enable AAA.

	Command	Purpose
Step 3	<b>aaa authentication dot1x {default} method1 [method2...]</b>	Create an 802.1x authentication method list.  To create a default list that is used when a named list is <i>not</i> specified in the <b>authentication</b> command, use the <b>default</b> keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.  Enter at least one of these keywords: <ul style="list-style-type: none"> <li>• <b>group radius</b>—Use the list of all RADIUS servers for authentication.</li> <li>• <b>none</b>—Use no authentication. The client is automatically authenticated by the switch without using the information supplied by the client.</li> </ul>
Step 4	<b>dot1x system-auth-control</b>	Enable 802.1x authentication globally on the switch.
Step 5	<b>aaa authorization network {default} group radius</b>	(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.  <b>Note</b> For per-user ACLs, single-host mode must be configured. This setting is the default.
Step 6	<b>interface interface-id</b>	Specify the port connected to the client that is to be enabled for 802.1x authentication, and enter interface configuration mode.
Step 7	<b>dot1x port-control auto</b>	Enable 802.1x authentication on the port.  For feature interaction information, see the “ <a href="#">802.1x Configuration Guidelines</a> ” section on page 10-10.
Step 8	<b>end</b>	Return to privileged EXEC mode.
Step 9	<b>show dot1x</b>	Verify your entries.
Step 10	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## Configuring 802.1x Accounting

Enabling AAA system accounting with 802.1x accounting allows system reload events to be sent to the accounting RADIUS server for logging. The server can then infer that all active 802.1x sessions are closed.

Because RADIUS uses the unreliable UDP transport protocol, accounting messages might 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, this system message appears:

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

When the stop message is not sent successfully, this message 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.
```

**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.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x accounting after AAA is enabled on your switch. This procedure is optional.

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Specify the port to be configured, and enter interface configuration mode.
Step 3	<b>aaa accounting dot1x default start-stop group radius</b>	Enable 802.1x accounting using the list of all RADIUS servers.
Step 4	<b>aaa accounting system default start-stop group radius</b>	(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>show running-config</b>	Verify your entries.
Step 7	<b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

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

This example shows how to configure 802.1x accounting. The first command configures the RADIUS server, specifying 1813 as the UDP port for accounting:

```
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
```

## 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 802.1x statistics for a specific interface, use the **show dot1x statistics interface *interface-id*** privileged EXEC command.

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

For detailed information about the fields in these displays, refer to the command reference for this release.

