



Configuring 802.1X Port-Based Authentication

This chapter describes how to configure IEEE 802.1X port-based authentication on your Catalyst 3550 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 9-1](#)
- [Configuring 802.1X Authentication, page 9-8](#)
- [Displaying 802.1X Statistics and Status, page 9-17](#)

Understanding 802.1X Port-Based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. 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) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

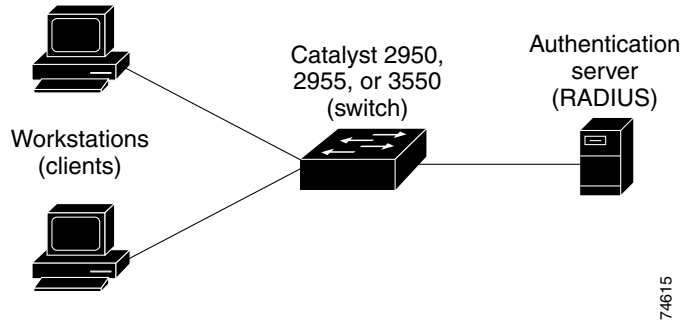
These sections describe 802.1X port-based authentication:

- [Device Roles, page 9-2](#)
- [Authentication Initiation and Message Exchange, page 9-3](#)
- [Ports in Authorized and Unauthorized States, page 9-4](#)
- [Voice VLAN Ports, page 9-5](#)
- [Using 802.1X with Port Security, page 9-5](#)
- [Using 802.1X with Per-User ACLs, page 9-6](#)
- [Using 802.1X with VLAN Assignment, page 9-7](#)
- [Supported Topologies, page 9-7](#)

Device Roles

With 802.1X port-based authentication, the devices in the network have specific roles as shown in Figure 9-1.

Figure 9-1 802.1X 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 Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- *Switch* (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 3550 multilayer switch, the Catalyst 2950 switch, 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.



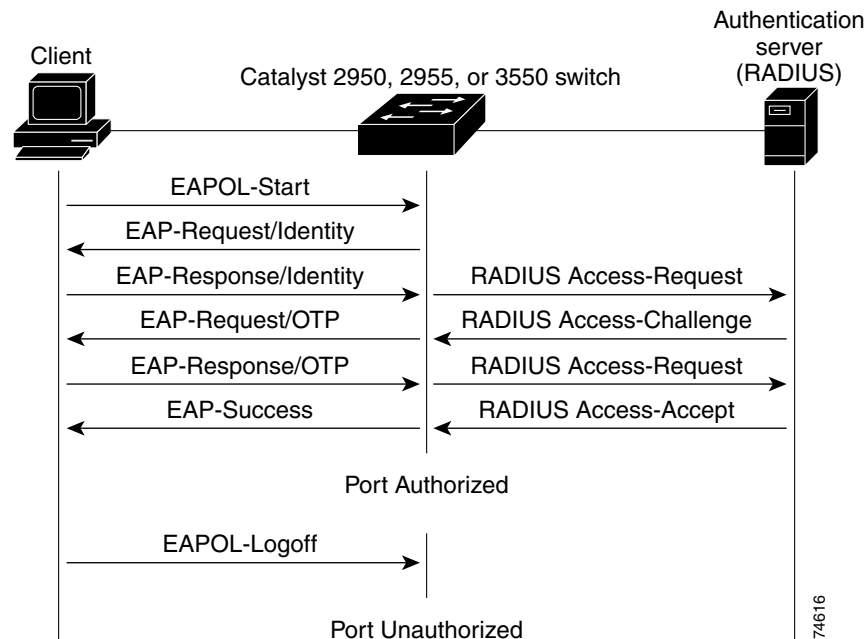
Note

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 9-4.

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 9-4.

The specific exchange of EAP frames depends on the authentication method being used. [Figure 9-2](#) shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 9-2 Message Exchange



74616

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.

Voice VLAN Ports

Multiple VLAN access ports (MVAPs) are ports that belong to two VLANs. This configuration allows the separating of voice traffic and the data traffic onto different VLANs. A switch port configured with a voice VLAN has separate VLANs configured for carrying:

- The voice traffic to and from the IP phone.
- The data traffic to and from the workstation connected to the switch through the IP phone.

Thus, each port configured for voice VLAN is associated with a port VLAN identifier (PVID) which is the native VLAN of the port, and a voice VLAN identifier (VVID) that is used to configure the IP phone connected to the port.

When 802.1X is enabled on a port that has a voice VLAN, the VLAN remains down on the port (equivalent to an unauthenticated state) until a CDP message is received from an IP phone. The VLAN then becomes active, allowing the phone to work independently of 802.1X authentication. The VLAN becomes inactive on the port if the CDP entry times out or if it is cleared by using the **cdp clear table** privileged EXEC command.

A workstation connected to the port uses the PVID and is authenticated through 802.1X as usual. The IP phone has access to the VVID for its voice traffic irrespective of the authorized or unauthorized state of the port.

Only one client is allowed on the voice VLAN other workstations or IP phones are blocked. When you enable the multiple-hosts mode, when an 802.1X user is authenticated on the primary VLAN, additional clients on the voice VLAN are unrestricted after 802.1X authentication succeeds on the primary VLAN.

When 802.1X is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

Using 802.1X with Port Security

You can enable an 802.1X port for port security by using the **dot1x multiple-hosts** interface configuration command. You must also configure port security on the port by using the **switchport port-security** interface configuration command. With the multiple-hosts mode enabled, 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 multiple-host 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 have 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. In this case, you should enable periodic reauthentication with a shorter time period than the port security aging time.

The port security violation modes determine the action for security violations. See the [“Security Violations” section on page 20-8](#) for more information.

- When the 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.

See the “[Enabling Multiple Hosts](#)” section on page 9-16, and the “[Configuring Port Security](#)” section on page 20-7 for more information about enabling 802.1X and port security on your switch.

Using 802.1X with Per-User ACLs

You can enable per-user ACLs to provide different levels of network access and service to an 802.1X-authenticated user. The per-user ACL attributes are retrieved from the RADIUS server and are applied for the duration of the user session.

The switch supports only one type of per-user ACL, router ACLs or port ACLs. Router ACLs apply to Layer 3 interfaces, and port ACLs apply to Layer 2 or Layer 3 interfaces. If one port is configured with a port-based ACL, the switch rejects any attempt to configure a router-based ACL. In contrast, if one port has a router-based ACL, the switch rejects any attempt to configure a port-based ACL. To avoid configuration conflicts, you should carefully plan the user profiles stored on the RADIUS server.

Only one 802.1X-authenticated user is supported on a port. If the multiple-hosts mode is enabled on the port, the per-user ACL attribute is disabled for the associated port.

QoS maps and VLAN maps are not supported for per-user ACLs.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are `inacl#<n>` for ingress direction and `outacl#<n>` for egress direction. MAC ACLs are only supported in the ingress direction.

Use only extended ACL syntax style to define the per-user configuration stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if you use the Filter-Id attribute, it can point to a standard ACL.

You can use the Filter-Id attribute to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by `.in` or `.out` for ingress filtering or egress filtering. If the RADIUS server does not allow `.in` or `.out` syntax, the access list is applied to the outbound ACL by default. The switch supports IP standard and IP extended access lists, number 1 to 199 and 1300 to 2699.

See the “[Configuring the Switch to Use Vendor-Specific RADIUS Attributes](#)” section on page 8-29 for examples of vendor-specific attributes and [Chapter 27, “Configuring Network Security with ACLs”](#) for more information about configuring ACLs.

To configure per-user ACLs, you need to:

- Enable AAA authentication
- Enable AAA authorization using the **network** and **config-commands** keywords to allow interface configuration from the RADIUS server
- Enable 802.1X
- Configure the user profile and VSAs on the RADIUS server
- Disable the 802.1X multiple-hosts mode on the port

Using 802.1X with VLAN Assignment

You can use VLAN assignment to limit network access for certain users. With 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 user.

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 AAA authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If authorization is enabled but the VLAN information from the server is not valid, the port remains down in the unauthenticated state. This prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error.

Configuration errors could include specifying a VLAN for a routed port, a malformed VLAN ID, a non-existent or internal (routed port) VLAN id, or attempting assignment to a voice VLAN ID.

- If authorization is enabled and all information from the server is valid, the port is placed in the specified VLAN after successful authentication.
- 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, it is returned to the configured access VLAN.

To configure VLAN assignment you need to:

- Enable AAA
- Enable 802.1X
- 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

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

See the “[Configuring the Switch to Use Vendor-Specific RADIUS Attributes](#)” section on page 8-29 for examples of vendor-specific attributes.

Supported Topologies

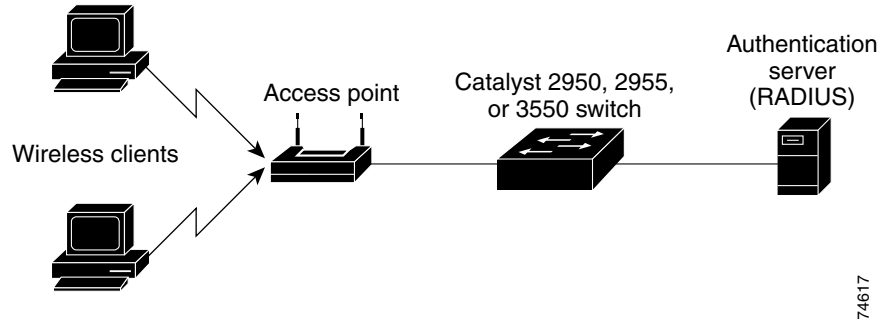
The 802.1X port-based authentication is supported in two topologies:

- Point-to-point
- Wireless LAN

In a point-to-point configuration (see [Figure 9-1 on page 9-2](#)), 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 9-3 shows 802.1X port-based authentication in a wireless LAN. The 802.1X port is configured as a multiple-host 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 9-3 Wireless LAN Example



74617

Configuring 802.1X Authentication

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

- [Default 802.1X Configuration, page 9-9](#)
- [802.1X Configuration Guidelines, page 9-10](#)
- [Enabling 802.1X Authentication, page 9-10](#) (required)
- [Configuring the Switch-to-RADIUS-Server Communication, page 9-12](#) (required)
- [Enabling Periodic Re-Authentication, page 9-13](#) (optional)
- [Manually Re-Authenticating a Client Connected to a Port, page 9-14](#) (optional)
- [Changing the Quiet Period, page 9-14](#) (optional)
- [Changing the Switch-to-Client Retransmission Time, page 9-15](#) (optional)
- [Setting the Switch-to-Client Frame-Retransmission Number, page 9-15](#) (optional)
- [Enabling Multiple Hosts, page 9-16](#) (optional)
- [Resetting the 802.1X Configuration to the Default Values, page 9-17](#) (optional)

Default 802.1X Configuration

Table 9-1 shows the default 802.1X configuration.

Table 9-1 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 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.
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).
Multiple host support	Disabled.
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 some configuration guidelines and operating characteristics of 802.1X authentication:

- When 802.1X is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- The 802.1X protocol is supported on both Layer 2 static-access ports and Layer 3 routed 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 port—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error message appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
 - Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1X on a port that is a SPAN or RSPAN destination or reflector port. However, 802.1X is disabled until the port is removed as a SPAN or RSPAN destination or reflector port. You can enable 802.1X on a SPAN or RSPAN source port.
- If you try to enable 802.1X on a secure port without enabling the multiple-hosts mode, the switch returns an error message, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port without enabling the multiple-hosts mode, the switch returns an error message, and the security settings are not changed.
- When 802.1X is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.

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 per-user ACLs and VLAN assignment, you need to 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	configure terminal	Enter global configuration mode.
Step 2	aaa new-model	Enable AAA.
Step 3	aaa authentication dot1x {default} method1 [method2...]	<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 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.</p> <p>Enter at least one of these keywords:</p> <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.
Step 4	aaa authorization network {default} group radius	<p>(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.</p> <p>Note To configure per-user ACLs, multiple-hosts mode must be disabled.</p>
Step 5	aaa authorization config-commands	(Optional) Configure the switch to allow per-user ACLs by enabling configuration mode commands.
Step 6	interface interface-id	Enter interface configuration mode, and specify the interface connected to the client that is to be enabled for 802.1X authentication.
Step 7	dot1x port-control auto	<p>Enable 802.1X authentication on the interface.</p> <p>For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports, see the “802.1X Configuration Guidelines” section on page 9-10.</p>
Step 8	end	Return to privileged EXEC mode.
Step 9	show dot1x	<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 auto or to force-unauthorized.</p>
Step 10	copy running-config startup-config	(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} method1 [method2...]** global configuration command. To disable 802.1X AAA authorization, use the **no aaa authorization** global configuration command. To disable 802.1X authentication, use the **dot1x port-control force-authorized** or the **no dot1x port-control** interface configuration command.

This example shows how to enable AAA and 802.1X on Fast Ethernet port 0/1:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
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	configure terminal	Enter global configuration mode.
Step 2	radius-server host { <i>hostname</i> <i>ip-address</i> } auth-port <i>port-number</i> key <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 auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. The default is 1812.</p> <p>For key <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>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, re-enter this command.</p>
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(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 8-29.

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.

Automatic 802.1X client re-authentication is a global setting and cannot be set for clients connected to individual ports. To manually re-authenticate the client connected to a specific port, see the “[Manually Re-Authenticating a Client Connected to a Port](#)” section on page 9-14.

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:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot1x re-authentication	Enable periodic re-authentication of the client, which is disabled by default.
Step 3	dot1x timeout re-authperiod <i>seconds</i>	Set the number of seconds between re-authentication attempts. The range is 1 to 4294967295; the default is 3600 seconds. This command affects the behavior of the switch only if periodic re-authentication is enabled.
Step 4	end	Return to privileged EXEC mode.
Step 5	show dot1x	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable periodic re-authentication, use the **no dot1x re-authentication** global configuration command. To return to the default number of seconds between re-authentication attempts, use the **no dot1x timeout re-authperiod** 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)# dot1x re-authentication
Switch(config)# dot1x timeout re-authperiod 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. If you want to enable or disable periodic re-authentication, see the “[Enabling Periodic Re-Authentication](#)” section on page 9-13.

This example shows how to manually re-authenticate the client connected to Fast Ethernet port 0/1:

```
Switch# dot1x re-authenticate interface fastethernet0/1
Starting reauthentication on 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:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot1x timeout quiet-period <i>seconds</i>	Set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 0 to 65535 seconds; the default is 60.
Step 3	end	Return to privileged EXEC mode.
Step 4	show dot1x	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

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

```
Switch(config)# 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:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	dot1x timeout tx-period <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 3	end	Return to privileged EXEC mode.
Step 4	show dot1x	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To return to the default retransmission time, use the **no dot1x timeout tx-period** global 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)# 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:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>dot1x max-req count</code>	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 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show dot1x</code>	Verify your entries.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

To return to the default retransmission number, use the **no dot1x max-req** global 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)# dot1x max-req 5
```

Enabling Multiple Hosts

You can attach multiple hosts to a single 802.1X-enabled port as shown in [Figure 9-3 on page 9-8](#). In this mode, only one of the attached hosts must be 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.

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

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

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

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

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x multiple-hosts
```

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	configure terminal	Enter global configuration mode.
Step 2	dot1x default	Reset the configurable 802.1X parameters to the default values.
Step 3	end	Return to privileged EXEC mode.
Step 4	show dot1x	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Displaying 802.1X Statistics and Status

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

