Configuring IEEE 802.1x Port-Based Authentication

This chapter describes how to configure IEEE 802.1x port-based authentication on the Cisco Industrial Ethernet 2000U Series Switches (IE 2000U).

As LANs extend to hotels, airports, and corporate lobbies and create insecure environments, 802.1x prevents unauthorized devices (clients) from gaining access to the network.

For complete syntax and usage information for the commands used in this chapter, see the documents listed in the "Related Documents" section on page 2-60.

This chapter consists of these sections:

- Information About 802.1x Port-Based Authentication, page 2-1
- Prerequisites, page 2-24
- Guidelines and Limitations, page 2-24
- Default Settings, page 2-26
- Configuring 802.1x Authentication, page 2-27
- Verifying Configuration, page 2-60
- Related Documents, page 2-60

Information About 802.1x Port-Based Authentication

The 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.

Note CDP and STP are supported by default on network node interfaces (NNIs). You can enable CDP and STP on enhanced network interfaces (ENIs). User network nodes (UNIs) do not support CDP or STP.

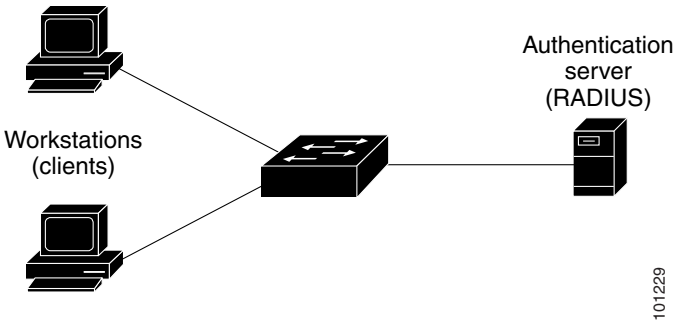
This section includes the following topics:

- Device Roles, page 2-2
- Authentication Process, page 2-3
- Authentication Initiation and Message Exchange, page 2-5
- Authentication Manager, page 2-7
- Ports in Authorized and Unauthorized States, page 2-8
- 802.1x Host Mode, page 2-9
- 802.1x Multiple-Authentication Mode, page 2-10
- MAC Move, page 2-10
- 802.1x Accounting, page 2-10
- 802.1x Accounting Attribute-Value Pairs, page 2-11
- 802.1x Readiness Check, page 2-12
- 802.1x Authentication with VLAN Assignment, page 2-12
- Using 802.1x Authentication with Per-User ACLs, page 2-13
- 802.1x Authentication with Downloadable ACLs and Redirect URLs, page 2-14
- VLAN ID-based MAC Authentication, page 2-15
- 802.1x Authentication with Guest VLAN, page 2-16
- 802.1x Authentication with Restricted VLAN, page 2-17
- 802.1x Authentication with Inaccessible Authentication Bypass, page 2-17
- 802.1x Authentication with Port Security, page 2-19
- 802.1x Authentication with Wake-on-LAN, page 2-20
- 802.1x Authentication with MAC Authentication Bypass, page 2-20
- 802.1x User Distribution, page 2-21
- Network Admission Control Layer 2 IEEE 802.1x Validation, page 2-22
- Flexible Authentication Ordering, page 2-22
- Open1x Authentication, page 2-22
- 802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT), page 2-23
- Common Session ID, page 2-24

Device Roles

With 802.1x port-based authentication, the devices in the network have specific roles as shown in Figure 2-1.

Figure 2-1 802.1x 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 802.1x specification.)
- *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 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.

Authentication Process

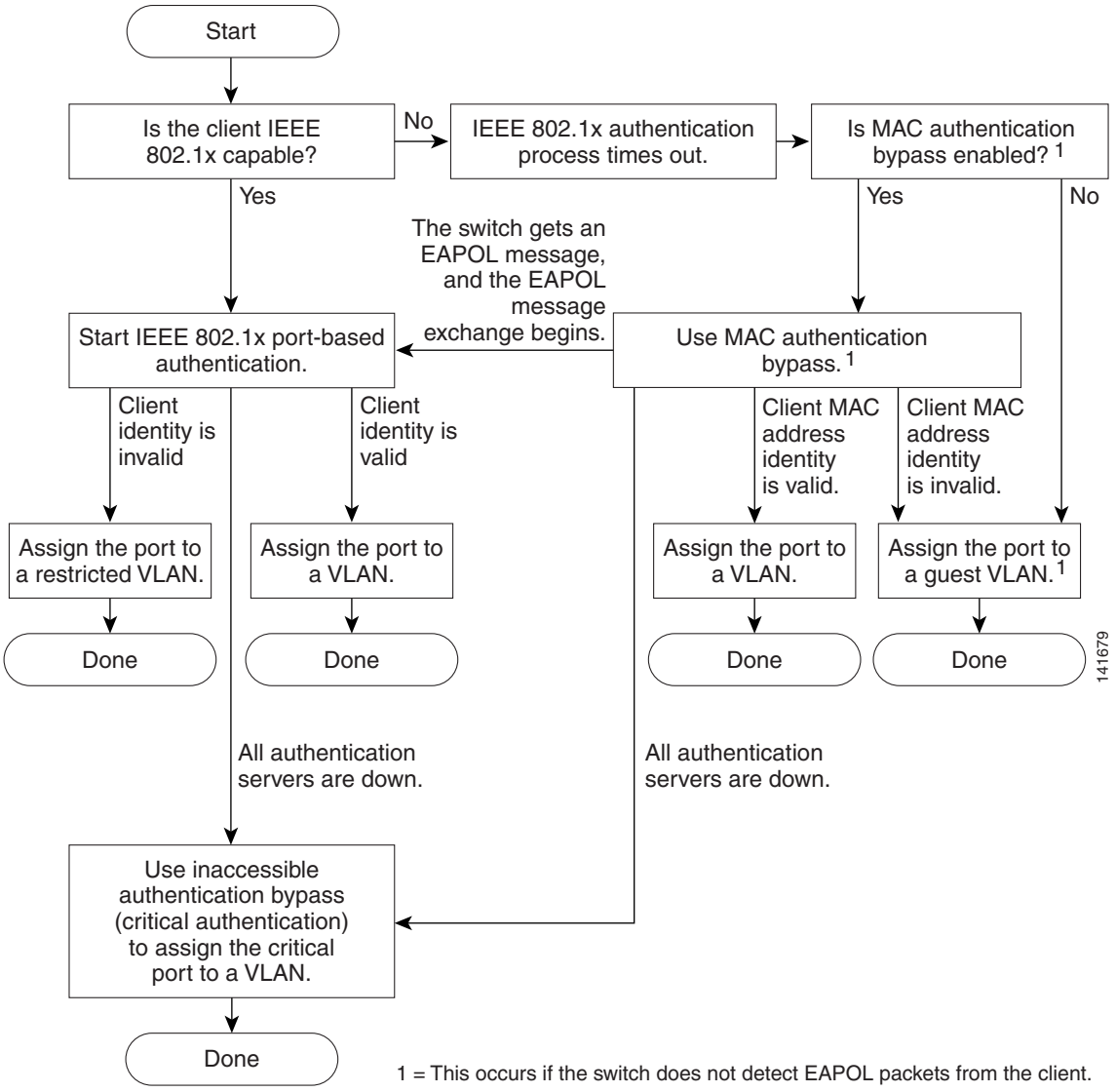
When 802.1x port-based authentication is enabled and the client supports 802.1x-compliant client software, these events occur:

- If the client identity is valid and the 802.1x authentication succeeds, the switch grants the client access to the network.
- If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can use the client MAC address for authorization. If the client MAC address is valid and the authorization succeeds, the switch grants the client access to the network. If the client MAC address is invalid and the authorization fails, the switch assigns the client to a guest VLAN that provides limited services if a guest VLAN is configured.

- If the switch gets an invalid identity from an 802.1x-capable client and a restricted VLAN is specified, the switch can assign the client to a restricted VLAN that provides limited services.
- If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN.

Note Inaccessible authentication bypass is also referred to as critical authentication or the AAA fail policy. See the "Configuring an AAA Fail Policy" section on page 3-16.

Figure 2-2 Authentication Flowchart



The switch re-authenticates a client when one of these situations occurs:

- Periodic re-authentication is enabled, and the re-authentication timer expires.

  You can configure the re-authentication timer to use a switch-specific value or to be based on values from the RADIUS server.

After 802.1x authentication using a RADIUS server is configured, the switch uses timers based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).

The Session-Timeout RADIUS attribute (Attribute[27]) specifies the time after which re-authentication occurs.

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during re-authentication. The actions are *Initialize* and *ReAuthenticate*. When the *Initialize* action is set (the attribute value is *DEFAULT*), the 802.1x session ends, and connectivity is lost during re-authentication. When the *ReAuthenticate* action is set (the attribute value is RADIUS-Request), the session is not affected during re-authentication.

- You manually re-authenticate the client by entering the **authentication periodic** interface configuration command.

Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the **authentication port-control auto** interface configuration command, the switch initiates authentication when the link state changes from down to up or periodically as long as the port remains up and unauthenticated. The switch sends an EAP-request/identity frame to the client to request its identity. Upon receipt of the frame, the client responds with an EAP-response/identity frame.

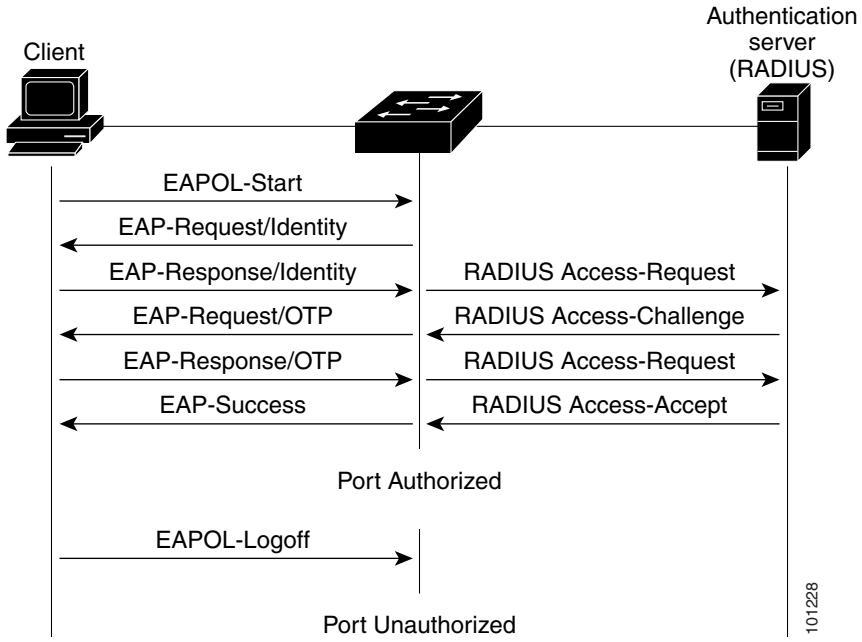
However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity.

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 2-8.

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 2-8.

The specific exchange of EAP frames depends on the authentication method being used. Figure 2-3 shows a message exchange initiated by the client when the client uses the One-Time-Password (OTP) authentication method with a RADIUS server.

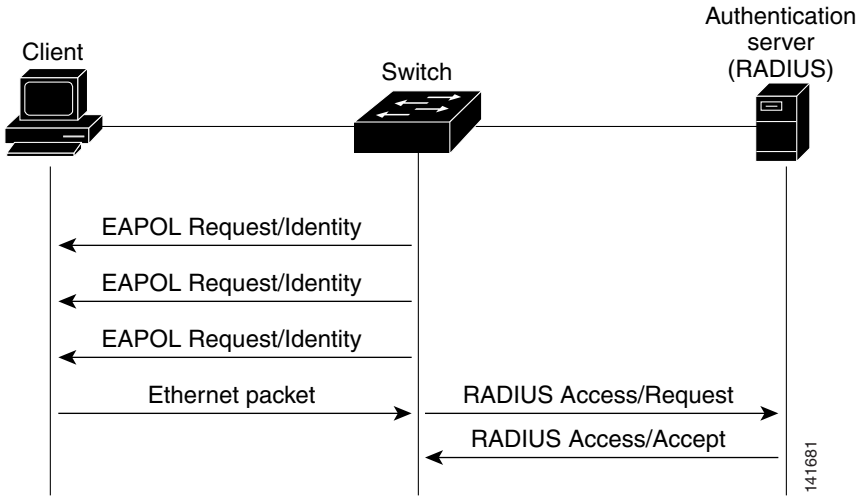
Figure 2-3 Message Exchange



If 802.1x authentication times out while waiting for an EAPOL message exchange and MAC authentication bypass is enabled, the switch can authorize the client when the switch detects an Ethernet packet from the client. The switch uses the MAC address of the client as its identity and includes this information in the RADIUS-access/request frame that is sent to the RADIUS server. After the server sends the switch the RADIUS-access/accept frame (authorization is successful), the port becomes authorized. If authorization fails and a guest VLAN is specified, the switch assigns the port to the guest VLAN. If the switch detects an EAPOL packet while waiting for an Ethernet packet, the switch stops the MAC authentication bypass process and stops 802.1x authentication.

Figure 2-4 shows the message exchange during MAC authentication bypass.

Figure 2-4 Message Exchange During MAC Authentication Bypass



Authentication Manager

This section contains the following topics:

- Port-Based Authentication Methods, page 2-7
- Per-User ACLs and Filter-IDs, page 2-8
- Authentication Manager CLI Commands, page 2-8

Note Catalyst switches that are running Cisco IOS Release 12.2(50)SE or later in a network support the same authorization methods as the IE 2000U switch.

Note The IE 2000U switch does not support multidomain authentication (MDA) or 802.1x authentication with voice VLAN ports.

Port-Based Authentication Methods

Table 2-1 802.1x Features

Authentication method	Mode		
	Single host	Multiple host	Multiple Authentication[1]
802.1x	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL	VLAN assignment	Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL
MAC authentication bypass	VLAN assignment Per-user ACL Filter-Id attribute Downloadable ACL Redirect URL	VLAN assignment	Per-user ACL Filter-Id attribute Downloadable[2]
Standalone web authentication[2]	Proxy ACL, Filter-Id attribute, downloadable ACL		
NAC Layer 2 IP validation	Filter-Id attribute Downloadable ACL Redirect URL	Filter-Id attribute Downloadable ACL Redirect URL	Filter-Id attribute Downloadable ACL Redirect URL
Web authentication as fallback method[2]	Proxy ACL Filter-Id attribute Downloadable ACL	Proxy ACL Filter-Id attribute Downloadable ACL	Proxy ACL Filter-Id attribute Downloadable ACL

1. Also referred to as *multiauth*.
2. For clients that do not support 802.1x authentication.

Per-User ACLs and Filter-IDs

You can only set **any** as the source in the ACL. **For any ACL configured for multiple-host mode, the source portion of statement must be *any*. (For example, permit icmp *any* host 10.10.1.1.)**

Authentication Manager CLI Commands

The authentication-manager interface-configuration commands control all the authentication methods, such as 802.1x, MAC authentication bypass, and web authentication. The authentication manager commands determine the priority and order of authentication methods applied to a connected host.

The authentication manager commands control generic authentication features, such as host-mode, violation mode, and the authentication timer. Generic authentication commands include the **authentication host-mode**, **authentication violation**, and **authentication timer** interface configuration commands.

802.1x-specific commands at the global configuration mode begin with **aaa authentication dot1x**. For example, the **authentication port-control auto** interface configuration command enables authentication on an interface. However, the **dot1x system-authentication control** global configuration command only globally enables or disables 802.1x authentication.

Note If 802.1x authentication is globally disabled, other authentication methods are still enabled on that port, such as web authentication.

The authentication manager commands provide the same functionality as earlier 802.1x commands.

For more information, see the *Cisco IOS Security Command Reference*.

Ports in Authorized and Unauthorized States

Depending on the switch port state, the switch can grant a client access to the network. The port starts in the *unauthorized* state. While in this state, the port disallows all incoming and outgoing traffic except for 802.1x, CDP, and STP packets. When a client is successfully authenticated, the port changes to the *authorized* state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1x connects 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 standard, 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 **authentication port-control** interface configuration command and these keywords:

- **force-authorized**—Disables 802.1x authentication and causes the port to change 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 port.

- **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 changes 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 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 change to the unauthorized state.

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

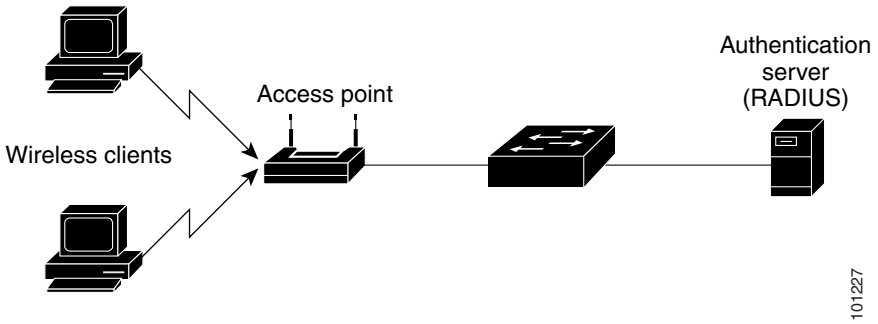
802.1x Host Mode

You can configure an 802.1x port for single-host or for multiple-hosts mode. In single-host mode (see Figure 2-1 on page 2-3), only one client can be connected to the 802.1x-enabled switch port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

In multiple-hosts mode, you can attach multiple hosts to a single 802.1x-enabled port. Figure 2-5 on page 2-9 shows 802.1x port-based authentication in a wireless LAN. In this mode, only one of the attached clients must be authorized for all clients to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), the switch denies network access to all of the attached clients. In this topology, the wireless access point is responsible for authenticating the clients attached to it, and it also acts as a client to the switch.

With 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.

Figure 2-5 Multiple Host Mode Example



802.1x Multiple-Authentication Mode

Multiple-authentication (multiauth) mode allows multiple authenticated clients on the data VLAN. When a hub or access point is connected to an 802.1x-enabled port, multiple-authentication mode provides enhanced security over multiple-hosts mode by requiring authentication of each connected client. For non-802.1x devices, you can use MAC authentication bypass or web authentication as the fallback method for individual host authentications to authenticate different hosts through different methods on a single port.

Note When a port is in multiple-authentication mode, the RADIUS-server-supplied VLAN assignment, guest VLAN, and the authentication-failed VLAN features do not activate.

For more information about critical authentication mode and the critical VLAN, see the "802.1x Authentication with Inaccessible Authentication Bypass" section on page 2-17.

For more information see the "Configuring 802.1x Accounting" section on page 2-41.

MAC Move

When a MAC address is authenticated on one switch port, that address is not allowed on another 802.1x port of the switch. If the switch detects that same MAC address on another 802.1x port, the address is not allowed.

There are situations where a MAC address might need to move from one port to another on the same switch. For example, when there is another device (for example a hub or an IP phone) between an authenticated host and a switch port, you might want to disconnect the host from the device and connect it directly to another port on the same switch.

You can globally enable MAC move so the device is re-authenticated on the new port. When a host moves to a second port, the session on the first port is deleted, and the host is re-authenticated on the new port.

MAC move is supported for all host modes. (The authenticated host can move to any port on the switch, no matter which host mode is enabled on the port.)

Note MAC move is not supported on port-security enabled 802.1x ports. If MAC move is globally configured on the switch and a port security-enabled host moves to an 802.1x-enabled port, a violation error occurs.

For more information see the "Enabling MAC Move" section on page 2-40.

802.1x Accounting

The 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.

802.1x Accounting Attribute-Value Pairs

The information sent to the RADIUS server is represented in the form of Attribute-Value (AV) pairs. These AV pairs provide data for different applications. (For example, a billing application might require information that is contained within the Acct-Input-Octets or the Acct-Output-Octets of a packet.)

AV pairs are automatically sent by a switch that is configured for 802.1x accounting. The switch sends these types of RADIUS accounting packets:

- START–Sent when a new user session starts
- INTERIM–Sent during an existing session for updates
- STOP–Sent when a session terminates

Table 2-2 lists the AV pairs that might be sent by the switch:

Table 2-2 Accounting AV Pairs

Attribute Number	AV Pair Name	START	INTERIM	STOP
Attribute[1]	User-Name	Always	Always	Always
Attribute[4]	NAS-IP-Address	Always	Always	Always
Attribute[5]	NAS-Port	Always	Always	Always
Attribute[8]	Framed-IP-Address	Never	Sometimes[1]	Sometimes[1]
Attribute[25]	Class	Always	Always	Always
Attribute[30]	Called-Station-ID	Always	Always	Always
Attribute[31]	Calling-Station-ID	Always	Always	Always
Attribute[40]	Acct-Status-Type	Always	Always	Always
Attribute[41]	Acct-Delay-Time	Always	Always	Always
Attribute[42]	Acct-Input-Octets	Never	Always	Always
Attribute[43]	Acct-Output-Octets	Never	Always	Always
Attribute[44]	Acct-Session-ID	Always	Always	Always
Attribute[45]	Acct-Authentic	Always	Always	Always
Attribute[46]	Acct-Session-Time	Never	Always	Always
Attribute[49]	Acct-Terminate-Cause	Never	Never	Always
Attribute[61]	NAS-Port-Type	Always	Always	Always

1. The Framed-IP-Address AV pair is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

You can see the AV pairs that are being sent by the switch by enabling the **debug radius accounting** or **debug aaa accounting** privileged EXEC commands. For more information about these commands, see the Cisco IOS Debug Command Reference.

For more information about AV pairs, see RFC 3580, "IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines."

802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable. You use an alternate authentication such as MAC authentication bypass or web authentication for devices that do not support 802.1x functionality.

This feature works only if the supplicant on the client supports a query with the NOTIFY EAP notification packet. The client must respond within the 802.1x timeout value.

For information on configuring the switch for the 802.1x readiness check, see the "Configuring 802.1x Readiness Check" section on page 2-28.

802.1x Authentication with VLAN Assignment

The switch supports 802.1x authentication with VLAN assignment. After 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, assigning the VLAN based on the username of the client connected to the switch port. You can use this feature to limit network access for certain users.

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. Recall that an access VLAN is a VLAN assigned to an access port. All packets sent from or received on this port belong to this VLAN.
- 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 specifying a VLAN for a routed port, a malformed VLAN ID, a nonexistent or internal (routed port) VLAN ID, an RSPAN VLAN, or a shut down or suspended VLAN. In the case of a multidomain host port, configuration errors can also be due to an attempted assignment of a data VLAN that matches the configured or assigned voice VLAN ID (or the reverse). Voice VLANs are not supported.
- If 802.1x authorization is enabled and all information from the RADIUS server is valid, the authorized device is placed in the specified VLAN.
- If 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.
- Enabling port security does not impact the RADIUS server-assigned VLAN behavior.
- If 802.1x authentication is disabled on the port, it is returned to the configured access VLAN.

When the port is in the force authorized, the force unauthorized, the unauthorized, or the shutdown state, it is put into 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 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 by using the **network** keyword to allow interface configuration from the RADIUS server.
- Enable 802.1x authentication. (The VLAN assignment feature is automatically enabled when you configure 802.1x authentication on an access port).
- Assign vendor-specific tunnel attributes on 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 1-44.

Using 802.1x Authentication with Per-User ACLs

You can enable per-user access control lists (ACLs) to provide different levels of network access and service to an 802.1x-authenticated user. When the RADIUS server authenticates a user connected to an 802.1x port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1x port for the duration of the user session. The switch removes the per-user ACL configuration when the session ends, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

You can configure router ACLs and input port ACLs on the same switch. However, a port ACL takes precedence over a router ACL. If you apply an input port ACL to an interface that belongs to a VLAN, the port ACL takes precedence over an input router ACL applied to the VLAN interface. The port ACL filters received packets. The router ACL filters received routed packets from other ports. The router ACL also filters sent routed packets. To avoid configuration conflicts, you should carefully plan the user profiles stored on the RADIUS server.

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 the ingress direction and `outacl#<n>` for the egress direction. MAC ACLs are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It does not support port ACLs in the egress direction on Layer 2 ports.

Use only the 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* for ingress filtering or *.out* for egress filtering. If the RADIUS server does not allow the *.in* or *.out* syntax, the access list is applied to the

outbound ACL by default. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered 1 to 199 and 1300 to 2699 (IP standard and IP extended ACLs).

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

The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.

For examples of vendor-specific attributes, see the "Configuring the Switch to Use Vendor-Specific RADIUS Attributes" section on page 1-44. For more information about configuring ACLs, see Chapter 6, "Configuring Network Security with ACLs."

To configure per-user ACLs, perform these tasks:

- Enable AAA authentication.
- Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server.
- Enable 802.1x authentication.
- Configure the user profile and VSAs on the RADIUS server.
- Configure the 802.1x port for single-host mode.

Note Per-user ACLs are supported only in single-host mode.

802.1x Authentication with Downloadable ACLs and Redirect URLs

You can download ACLs and redirect URLs from a RADIUS server to the switch during 802.1x authentication or MAC authentication bypass of the host. You can also download ACLs during web authentication.

Note A downloadable ACL is also referred to as a *dACL*.

If the host mode is in single-host or multiple-authentication mode, the switch modifies the source address of the ACL to be the host IP address.

You can apply the ACLs and redirect URLs to all the devices connected to the 802.1x-enabled port.

If no ACLs are downloaded during 802.1x authentication, the switch applies the static default ACL on the port to the host.

Note If a downloadable ACL or redirect URL is configured for a client on the authentication server, you must also configure a default port ACL on the connected client switch port.

Cisco Secure ACS and Attribute-Value Pairs for the Redirect URL

The switch uses these *cisco-av-pair* VSAs:

- url-redirect is the HTTP to HTTPS URL.
- url-redirect-acl is the switch ACL name or number.

The switch uses the CiscoSecure-Defined-ACL AV pair to intercept an HTTP or HTTPS request from the endpoint device. The switch then forwards the client web browser to the specified redirect address. The url-redirect AV pair on the Cisco Secure ACS contains the URL to which the web browser is redirected. The url-redirect-acl AV pair contains the name or number of an ACL that specifies the HTTP or HTTPS traffic to redirect. Traffic that matches a permit ACE in the ACL is redirected.

Note Define the URL redirect ACL and the default port ACL on the switch.

If a redirect URL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

Cisco Secure ACS and Attribute-Value Pairs for Downloadable ACLs

You can set the CiscoSecure-Defined-ACL Attribute-Value (AV) pair on the Cisco Secure ACS with the RADIUS cisco-av-pair vendor-specific attributes (VSAs). This pair specifies the names of the downloadable ACLs on the Cisco Secure ACS with the #ACL#-IP-name-number attribute, where:

- The *name* is the ACL name.
- The *number* is the version number (for example, 3f783768).

If a downloadable ACL is configured for a client on the authentication server, a default port ACL on the connected client switch port must also be configured.

If the default ACL is configured on the switch and the Cisco Secure ACS sends a host-access-policy to the switch, it applies the policy to traffic from the host connected to a switch port. If the policy does not apply, the switch applies the default ACL. If the Cisco Secure ACS sends the switch a downloadable ACL, this ACL takes precedence over the default ACL that is configured on the switch port. However, if the switch receives a host access policy from the Cisco Secure ACS but the default ACL is not configured, the authorization failure is declared.

For configuration details, see the "Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs" section on page 2-54.

VLAN ID-based MAC Authentication

You can use VLAN ID-based MAC authentication if you wish to authenticate hosts based on a static VLAN ID instead of a downloadable VLAN. When you have a static VLAN policy configured on your switch, VLAN information is sent to an IAS (Microsoft) RADIUS server along with the MAC address of each host for authentication. The VLAN ID configured on the connected port is used for MAC authentication. By using VLAN ID-based MAC authentication with an IAS server, you can have a fixed number of VLANs in the network.

The feature also limits the number of VLANs monitored and handled by STP. The network can be managed as a fixed VLAN.

Note This feature is not supported on the Cisco ACS server. (The ACS server ignores the sent VLAN-IDs for new hosts and only authenticates based on the MAC address.)

For configuration information, see the "Configuring VLAN ID-based MAC Authentication" section on page 2-57. Additional configuration is similar to MAC authentication bypass, as described in the "Configuring MAC Authentication Bypass" section on page 2-48.

802.1x Authentication with Guest VLAN

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

When you enable a guest VLAN on an 802.1x port, the switch assigns clients to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.

The switch maintains the EAPOL packet history. If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an 802.1x-capable supplicant, and the interface does not change to the guest VLAN state. EAPOL history is cleared if the interface link status goes down. If no EAPOL packet is detected on the interface, the interface changes to the guest VLAN state.

If devices send EAPOL packets to the switch during the lifetime of the link, the switch does not allow clients that fail authentication access to the guest VLAN.

If the switch is trying to authorize an 802.1x-capable voice device and the AAA server is unavailable, the authorization attempt fails, but the detection of the EAPOL packet is saved in the EAPOL history. When the AAA server becomes available, the switch authorizes the voice device. However, the switch does not allow other devices access to the guest VLAN. To prevent this situation, use one of these command sequences:

- Enter the **dot1x guest-vlan supplicant** global configuration command to allow access to the guest VLAN.
- Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to restart the port.

Note If an EAPOL packet is detected after the interface has changed to the guest VLAN, the interface reverts to an unauthorized state, and 802.1x authentication restarts.

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

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

You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN. The guest VLAN feature is not supported on trunk ports; it is supported only on access ports.

The switch supports *MAC authentication bypass*. When MAC authentication bypass is enabled on an 802.1x port, the switch can authorize clients based on the client MAC address when 802.1x authentication times out while waiting for an EAPOL message exchange. After detecting a client on an 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is specified. For more information, see the "802.1x Authentication with MAC Authentication Bypass" section on page 2-20.

For more information, see the "Configuring a Guest VLAN" section on page 2-42.

802.1x Authentication with Restricted VLAN

You can configure a restricted VLAN (also referred to as an *authentication failed VLAN*) for each 802.1x port on a switch to provide limited services to clients that cannot access the guest VLAN. These clients are 802.1x-compliant and cannot access another VLAN because they fail the authentication process. A restricted VLAN allows users without valid credentials in an authentication server (typically, visitors to an enterprise) to access a limited set of services. The administrator can control the services available to the restricted VLAN.

Note You can configure a VLAN to be both the guest VLAN and the restricted VLAN if you want to provide the same services to both types of users.

Without this feature, the client attempts and fails authentication indefinitely, and the switch port remains in the spanning-tree blocking state. With this feature, you can configure the switch port to be in the restricted VLAN after a specified number of authentication attempts (the default value is 3 attempts).

The authenticator counts the failed authentication attempts for the client. When this count exceeds the configured maximum number of authentication attempts, the port moves to the restricted VLAN. The failed attempt count increments when the RADIUS server replies with either an *EAP failure* or an empty response without an EAP packet. When the port moves into the restricted VLAN, the failed attempt counter resets.

Users who fail authentication remain in the restricted VLAN until the next re-authentication attempt. A port in the restricted VLAN tries to re-authenticate at configured intervals (the default is 60 seconds). If re-authentication fails, the port remains in the restricted VLAN. If re-authentication is successful, the port moves either to the configured VLAN or to a VLAN sent by the RADIUS server. You can disable re-authentication. If you do this, the only way to restart the authentication process is for the port to receive a *link dow*n or *EAP logoff* event. We recommend that you keep re-authentication enabled if a client might connect through a hub. When a client disconnects from the hub, the port might not receive the *link down* or *EAP logoff* event.

After a port moves to the restricted VLAN, a simulated EAP success message is sent to the client. This prevents clients from indefinitely attempting authentication. Some clients (for example, devices running Windows XP) cannot implement DHCP without EAP success.

Restricted VLANs are supported only on 802.1x ports in single-host mode and on Layer 2 ports.

You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN. The restricted VLAN feature is not supported on trunk ports; it is supported only on access ports.

This feature works with port security. As soon as the port is authorized, a MAC address is provided to port security. If port security does not permit the MAC address or if the maximum secure address count is reached, the port becomes unauthorized and error disabled.

Other port security features such as dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on a restricted VLAN.

For more information, see the "Configuring a Restricted VLAN" section on page 2-43.

802.1x Authentication with Inaccessible Authentication Bypass

Use the inaccessible authentication bypass feature, also referred to as critical authentication or the AAA fail policy, when the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated. You can configure the switch to connect those hosts to critical ports.

When a new host tries to connect to the critical port, that host is moved to a user-specified access VLAN, the critical VLAN. The administrator gives limited authentication to the hosts.

When the switch tries to authenticate a host connected to a critical port, the switch checks the status of the configured RADIUS server. If a server is available, the switch can authenticate the host. However, if all the RADIUS servers are unavailable, the switch grants network access to the host and puts the port in the critical-authentication state, which is a special case of the authentication state.

Support on Multiple-Authentication Ports

To support inaccessible bypass on multiple-authentication (multiauth) ports, you can use the **authentication event server dead action reinitialize vlan** *vlan-id.* When a new host tries to connect to the critical port, that port is reinitialized and all the connected hosts are moved to the user-specified access VLAN.

The **authentication event server dead action reinitialize vlan** *vlan-id* interface configuration command is supported for all host modes.

Authentication Results

The behavior of the inaccessible authentication bypass feature depends on the authorization state of the port:

- If the port is unauthorized when a host connected to a critical port tries to authenticate and all servers are unavailable, the switch puts the port in the critical-authentication state in the RADIUS-configured or user-specified access VLAN.
- If the port is already authorized and re-authentication occurs, the switch puts the critical port in the critical-authentication state in the current VLAN, which might be the one previously assigned by the RADIUS server.
- If the RADIUS server becomes unavailable during an authentication exchange, the current exchange times out, and the switch puts the critical port in the critical-authentication state during the next authentication attempt.

You can configure the critical port to reinitialize hosts and move them out of the critical VLAN when the RADIUS server is again available. When this is configured, all critical ports in the critical-authentication state are automatically re-authenticated. For more information, see the *Cisco IOS Security Command Reference* and the "Configuring the Inaccessible Authentication Bypass Feature" section on page 2-44.

Feature Interactions

Inaccessible authentication bypass interacts with these features:

- Guest VLAN—Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on an 8021.x port, the features interact as follows:
  - If at least one RADIUS server is available, the switch assigns a client to a guest VLAN when the switch does not receive a response to its EAP request/identity frame or when EAPOL packets are not sent by the client.
  - If all the RADIUS servers are not available and the client is connected to a critical port, the switch authenticates the client and puts the critical port in the critical-authentication state in the RADIUS-configured or user-specified access VLAN.

  - If all the RADIUS servers are not available and the client is not connected to a critical port, the switch might not assign clients to the guest VLAN if one is configured.
  - If all the RADIUS servers are not available and if a client is connected to a critical port and was previously assigned to a guest VLAN, the switch keeps the port in the guest VLAN.
- Restricted VLAN—If the port is already authorized in a restricted VLAN and the RADIUS servers are unavailable, the switch puts the critical port in the critical-authentication state in the restricted VLAN.
- 802.1x accounting—Accounting is not affected if the RADIUS servers are unavailable.
- Private VLAN—You can configure inaccessible authentication bypass on a private VLAN host port. The access VLAN must be a secondary private VLAN.
- Remote Switched Port Analyzer (RSPAN)—Do not configure an RSPAN VLAN as the RADIUS-configured or user-specified access VLAN for inaccessible authentication bypass.

802.1x Authentication with Port Security

You can configure an 802.1x port with port security in either single-host or multiple-hosts mode. (You also must 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 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 the 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 address is aged, its place in the secure host table can be taken by another host.

  If the security violation is caused by the first authenticated host, the port becomes error-disabled and immediately shuts down.

  The port security violation modes determine the action for security violations.
- When you manually remove an 802.1x client address from the port security table by using the **no switchport port-security mac-address** *mac-address* interface configuration command, you should re-authenticate the 802.1x client by using the **authentication periodic** interface configuration command.
- When an 802.1x client logs off, the port changes 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.
- You can configure the **authentication violation** interface configuration command so that a port shuts down, generates a syslog error, accepts, or discards packets from a new device when it connects to an IEEE 802.1x-enabled port or when the maximum number of allowed devices have been authenticated. For more information see the "Maximum Number of Allowed Devices Per Port"

section on page 2-25 and the *Cisco IOS Security Command Reference*.

802.1x Authentication with Wake-on-LAN

The 802.1x authentication with the wake-on-LAN (WoL) feature allows dormant PCs to be powered when the switch receives a specific Ethernet frame, known as the *magic packet.* You can use this feature in environments where administrators need to connect to systems that have been powered down.

When a host that uses WoL is attached through an 802.1x port and the host powers off, the 802.1x port becomes unauthorized. The port can only receive and send EAPOL packets, and WoL magic packets cannot reach the host. When the PC is powered off, it is not authorized, and the switch port is not opened.

When the switch uses 802.1x authentication with WoL, the switch forwards traffic to unauthorized 802.1x ports, including magic packets. While the port is unauthorized, the switch continues to block ingress traffic other than EAPOL packets. The host can receive packets but cannot send packets to other devices in the network.

Note If PortFast is not enabled on the port, the port is forced to the bidirectional state.

When you configure a port as unidirectional by using the **authentication control-direction in** interface configuration command, the port changes to the spanning-tree forwarding state. The port can send packets to the host but cannot receive packets from the host.

When you configure a port as bidirectional by using the **authentication control-direction both** interface configuration command, the port is access-controlled in both directions. The port does not receive packets from or send packets to the host.

802.1x Authentication with MAC Authentication Bypass

You can configure the switch to authorize clients based on the client MAC address by using the MAC authentication bypass feature. For example, you can enable this feature on 802.1x ports connected to devices such as printers.

If 802.1x authentication times out while waiting for an EAPOL response from the client, the switch tries to authorize the client by using MAC authentication bypass.

When the MAC authentication bypass feature is enabled on an 802.1x port, the switch uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. After detecting a client on an 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the switch grants the client access to the network. If authorization fails, the switch assigns the port to the guest VLAN if one is configured.

If an EAPOL packet is detected on the interface during the lifetime of the link, the switch determines that the device connected to that interface is an 802.1x-capable supplicant and uses 802.1x authentication (not MAC authentication bypass) to authorize the interface. EAPOL history is cleared if the interface link status goes down.

If the switch already authorized a port by using MAC authentication bypass and detects an 802.1x supplicant, the switch does not unauthorize the client connected to the port. When re-authentication occurs, the switch uses 802.1x authentication as the preferred re-authentication process if the previous session ended because the Termination-Action RADIUS attribute value is DEFAULT.

Clients that were authorized with MAC authentication bypass can be re-authenticated. The re-authentication process is the same as that for clients that were authenticated with 802.1x. During re-authentication, the port remains in the previously assigned VLAN. If re-authentication is successful, the switch keeps the port in the same VLAN. If re-authentication fails, the switch assigns the port to the guest VLAN, if one is configured.

If re-authentication is based on the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]) and if the Termination-Action RADIUS attribute (Attribute [29]) action is *Initialize,* (the attribute value is *DEFAULT*), the MAC authentication bypass session ends, and connectivity is lost during re-authentication. If MAC authentication bypass is enabled and the 802.1x authentication times out, the switch uses the MAC authentication bypass feature to initiate re-authorization. For more information about these AV pairs, see RFC 3580, "802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines."

MAC authentication bypass interacts with the features:

- 802.1x authentication—You can enable MAC authentication bypass only if 802.1x authentication is enabled on the port.
- Guest VLAN—If a client has an invalid MAC address identity, the switch assigns the client to a guest VLAN if one is configured.
- Restricted VLAN—This feature is not supported when the client connected to an 802.1x port is authenticated with MAC authentication bypass.
- Port security—See the "802.1x Readiness Check" section on page 2-12.
- VLAN Membership Policy Server (VMPS)—802.1x and VMPS are mutually exclusive.
- Private VLAN—You can assign a client to a private VLAN.

802.1x User Distribution

You can configure 802.1x user distribution to load-balance users with the same group name across multiple different VLANs.

The VLANs are either supplied by the RADIUS server or configured through the switch CLI under a VLAN group name.

- Configure the RADIUS server to send more than one VLAN name for a user. The multiple VLAN names can be sent as part of the response to the user. The 802.1x user distribution tracks all the users in a particular VLAN and achieves load balancing by moving the authorized user to the least populated VLAN.
- Configure the RADIUS server to send a VLAN group name for a user. The VLAN group name can be sent as part of the response to the user. You can search for the selected VLAN group name among the VLAN group names that you configured by using the switch CLI. If the VLAN group name is found, the corresponding VLANs under this VLAN group name are searched to find the least populated VLAN. Load balancing is achieved by moving the corresponding authorized user to that VLAN.

Note The RADIUS server can send the VLAN information in any combination of VLAN IDs, VLAN names, or VLAN groups.

Network Admission Control Layer 2 IEEE 802.1x Validation

The switch supports the Network Admission Control (NAC) Layer 2 802.1x validation, which checks the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access. With NAC Layer 2 802.1x validation, you can do these tasks:

- Download the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute[29]) from the authentication server.
- Set the number of seconds between re-authentication attempts as the value of the Session-Timeout RADIUS attribute (Attribute[27]) and get an access policy against the client from the RADIUS server.
- Set the action to be taken when the switch tries to re-authenticate the client by using the Termination-Action RADIUS attribute (Attribute[29]). If the value is *DEFAULT* or is not set, the session ends. If the value is RADIUS-Request, the re-authentication process starts.
- See the NAC posture token, which shows the posture of the client, by using the **show authentication** command in user EXEC or privileged EXEC mode.
- Configure secondary private VLANs as guest VLANs.

Configuring NAC Layer 2 802.1x validation is similar to configuring 802.1x port-based authentication except that you must configure a posture token on the RADIUS server. For information about configuring NAC Layer 2 802.1x validation, see the "Configuring NAC Layer 2 IEEE 802.1x Validation" section on page 2-50 and the "Configuring Periodic Re-Authentication" section on page 2-36.

For more information about NAC, see the *Network Admission Control Configuration Guide, Cisco IOS Release 15MT*.

For more configuration information, see the "Authentication Manager" section on page 2-7.

Flexible Authentication Ordering

You can use flexible authentication ordering to configure the order of methods that a port uses to authenticate a new host. MAC authentication bypass and 802.1x can be the primary or secondary authentication methods, and web authentication can be the fallback method if either or both of those authentication attempts fail. For more information see the "Configuring Flexible Authentication Ordering" section on page 2-58.

Open1x Authentication

Open1x authentication allows a device access to a port before that device is authenticated. When open authentication is configured, a new host on the port can only send traffic to the switch. After the host is authenticated, the policies configured on the RADIUS server are applied to that host.

You can configure open authentication with these scenarios:

- Single-host mode with open authentication–Only one user is allowed network access before and after authentication.
- Multiple-hosts mode with open authentication–Any host can access the network.
- Multiple-authentication mode with open authentication–Similar to MDA, except multiple hosts can be authenticated.

For more information see the "Configuring 802.1x Accounting" section on page 2-41.

Using Voice Aware 802.1x Security

You use the voice aware 802.1x security feature to configure the switch to disable only the data VLAN on which a security violation occurs rather than to shut down the entire port. You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN shuts down the data VLAN.

For information on configuring voice aware 802.1x security, see the "Configuring Voice Aware 802.1x Security" section on page 2-31.

802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)

The Network Edge Access Topology (NEAT) feature extends identity to areas outside the wiring closet (such as conference rooms), allowing any type of device to authenticate on the port.

- 802.1x switch supplicant: You can configure a switch to act as a supplicant to another switch by using the 802.1x supplicant feature. This configuration is helpful in a scenario, where, for example, a switch is outside a wiring closet and is connected to an upstream switch through a trunk port. A switch configured with the 802.1x switch supplicant feature authenticates with the upstream switch for secure connectivity.

  Once the supplicant switch authenticates successfully the port mode changes from access to trunk.

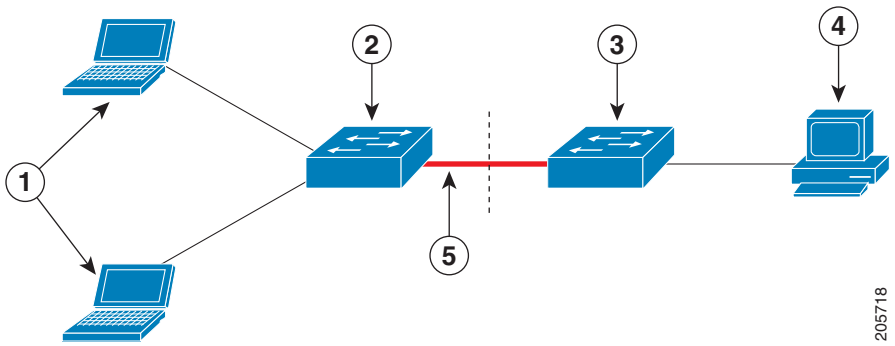
- If the access VLAN is configured on the authenticator switch, it becomes the native VLAN for the trunk port after successful authentication.

You can enable multiple-authentication mode on the authenticator switch interface that connects to one or more supplicant switches. Multiple-host mode is not supported on the authenticator switch interface.

Use the **dot1x supplicant force-multicast** global configuration command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

- Host Authorization: Ensures that only traffic from authorized hosts (connecting to the switch with supplicant) is allowed on the network. The switches use Client Information Signalling Protocol (CISP) to send the MAC addresses connecting to the supplicant switch to the authenticator switch, as shown in Figure 2-6.
- Auto enablement: Automatically enables trunk configuration on the authenticator switch, allowing user traffic from multiple VLANs coming from supplicant switches. Configure the cisco-av-pair as *device-traffic-class=switch* at the ACS. (You can configure this under the *group* or the *user* settings.)

Figure 2-6 Authenticator and Supplicant Switch using CISP



	Workstations (clients)		Supplicant switch (outside wiring closet)
	Authenticator switch		Access control server (ACS)
	Trunk port		

Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32-bit integer
- The session start time stamp (a 32-bit integer)

This example shows how the session ID appears in the output of the show authentication command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions
Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

Prerequisites

Be sure to review the Guidelines and Limitations section and the Before You Begin section within each configuration section before configuring a feature.

Guidelines and Limitations

- 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 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, an error message appears, and 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—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 or RSPAN destination port. However, 802.1x is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable 802.1x on a SPAN or RSPAN source port.

- You can configure any VLAN except an RSPAN VLAN or a private VLAN.
- The 802.1x with VLAN assignment feature is not supported on private-VLAN ports, trunk ports, or ports with dynamic-access port assignment through a VMPS.
- You can configure 802.1x on a private-VLAN port, but do not configure 802.1x with port security on private-VLAN ports.
- 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.

Maximum Number of Allowed Devices Per Port

This is the maximum number of devices allowed on an 802.1x-enabled port:

- In single-host mode, only one device is allowed on the access VLAN.
- In multiple-hosts mode, only one 802.1x supplicant is allowed on the port, but an unlimited number of non-802.1x hosts are allowed on the access VLAN.

802.1x User Distribution

- Confirm that at least one VLAN is mapped to the VLAN group.
- You can map more than one VLAN to a VLAN group.
- You can modify the VLAN group by adding or deleting a VLAN.
- When you clear an existing VLAN from the VLAN group name, none of the authenticated ports in the VLAN are cleared, but the mappings are removed from the existing VLAN group.
- If you clear the last VLAN from the VLAN group name, the VLAN group is cleared.
- You can clear a VLAN group even when the active VLANs are mapped to the group. When you clear a VLAN group, none of the ports or users that are in the authenticated state in any VLAN within the group are cleared, but the VLAN mappings to the VLAN group are cleared.

For more information, see the "Configuring 802.1x User Distribution" section on page 2-49.

NEAT

- You can configure NEAT ports with the same configurations as the other authentication ports. When the supplicant switch authenticates, the port mode changes from access to trunk based on the switch vendor-specific attributes (VSAs). (*device-traffic-class=switch*).

- The VSA changes the authenticator switch port mode from access to trunk and enables 802.1x trunk encapsulation. The access VLAN, if any, is then converted to a native trunk VLAN. The VSA does not change any of the port configurations on the supplicant.

For more information, see the "Configuring an Authenticator and a Supplicant Switch with NEAT" section on page 2-52.

Default Settings

Feature	Default Setting
AAA	Disabled.
RADIUS server • IP address • UDP authentication port • Key	 • None specified. • 1812. • None specified.
Switch 802.1x enable state	Disabled.
Per-port 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.
Re-authentication number	2 times (number of times that the switch restarts the authentication process before the port changes to the unauthorized state).
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.

Feature	Default Setting
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.) You can change this timeout period by using the authentication timer interface configuration command.

Configuring 802.1x Authentication

This section includes the following topics:

- Configuring 802.1x Readiness Check, page 2-28 (optional)
- Configuring the Switch-to-RADIUS Server Communication, page 2-29 (required)
- Configuring Voice Aware 802.1x Security, page 2-31 (optional)
- Configuring 802.1x Violation Modes, page 2-32
- Configuring 802.1x Authentication, page 2-33
- Configuring 802.1x Accounting, page 2-41 (optional)
- Configuring Periodic Re-Authentication, page 2-36 (optional)
- Manually Re-Authenticating a Client Connected to a Port, page 2-37 (optional)
- Changing the Quiet Period, page 2-37 (optional)
- Changing the Switch-to-Client Retransmission Time, page 2-38 (optional)
- Setting the Switch-to-Client Frame-Retransmission Number, page 2-38 (optional)
- Setting the Re-Authentication Number, page 2-39 (optional)
- Enabling MAC Move, page 2-40 (optional)
- Configuring 802.1x Accounting, page 2-41 (optional)
- Configuring a Guest VLAN, page 2-42
- Configuring a Restricted VLAN, page 2-43
- Configuring the Inaccessible Authentication Bypass Feature, page 2-44
- Configuring 802.1x Authentication with Wake-on-LAN, page 2-47
- Configuring MAC Authentication Bypass, page 2-48
- Configuring 802.1x User Distribution, page 2-49 (optional)
- Configuring NAC Layer 2 IEEE 802.1x Validation, page 2-50 (optional)
- Resetting the 802.1x Authentication Configuration to the Default Values, page 2-51 (optional)
- Disabling 802.1x Authentication on the Port, page 2-52 (optional)
- Configuring an Authenticator and a Supplicant Switch with NEAT, page 2-52 (optional)

- Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs, page 2-54 (optional)
- Configuring VLAN ID-based MAC Authentication, page 2-57 (optional)
- Configuring Flexible Authentication Ordering, page 2-58 (optional)
- Configuring Open1x, page 2-58 (optional)

Configuring 802.1x Readiness Check

The 802.1x readiness check monitors 802.1x activity on all the switch ports and displays information about the devices connected to the ports that support 802.1x. You can use this feature to determine if the devices connected to the switch ports are 802.1x-capable.

The 802.1x readiness check is allowed on all ports that can be configured for 802.1x. The readiness check is not available on a port that is configured as **authentication port-control force-unauthorized**.

BEFORE YOU BEGIN

Follow these guidelines to enable the readiness check on the switch:

- The readiness check is typically used before 802.1x is enabled on the switch.
- If you use the **dot1x test eapol-capable** privileged EXEC command without specifying an interface, all the ports on the switch stack are tested.
- When you configure the **dot1x test eapol-capable** command on an 802.1x-enabled port and the link comes up, the port queries the connected client about its 802.1x capability. When the client responds with a notification packet, it is 802.1x-capable. A syslog message is generated if the client responds within the timeout period. If the client does not respond to the query, the client is not 802.1x-capable. No syslog message is generated.
- The readiness check can be sent on a port that handles multiple hosts (for example, a PC that is connected to an IP phone). A syslog message is generated for each of the clients that respond to the readiness check within the timer period.

DETAILED STEPS

	Command	Purpose
Step 1	**dot1x test eapol-capable** [**interface** *interface-id*]	Enable the 802.1x readiness check on the switch. (Optional) For *interface-id* specify the port on which to check for IEEE 802.1x readiness. **Note** If you omit the optional **interface** keyword, all interfaces on the switch are tested.
Step 1	**configure terminal**	(Optional) Enter global configuration mode.
Step 2	**dot1x test timeout** *timeout*	(Optional) Configure the timeout used to wait for the EAPOL response. The range is from 1 to 65535 seconds. The default is 10 seconds.
Step 3	**end**	(Optional) Return to privileged EXEC mode.
Step 4	**show running-config**	(Optional) Verify your modified timeout values.

EXAMPLE

This example shows how to enable a readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is 802.1x-capable.

```
switch# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

Configuring the Switch-to-RADIUS Server Communication

RADIUS security servers are identified by their hostname or IP address, hostname 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 failover backup to the first one. The RADIUS host entries are tried in the order that they were configured.

BEFORE YOU BEGIN

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, see the RADIUS server documentation.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	Configure the RADIUS server parameters. For *hostname* | *ip-address,* specify the hostname or IP address of the remote RADIUS server. For **auth-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1812. The range is 0 to 65536. For **key** *string*, 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. **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. If you want to use multiple RADIUS servers, reenter this command.
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.

EXAMPLE

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 1-43.

Configuring Voice Aware 802.1x Security

You use the voice aware 802.1x security feature to configure the switch to disable only the data VLAN on which a security violation occurs rather than to shut down the entire port. You can use this feature in IP phone deployments where a PC is connected to the IP phone. A security violation found on the data VLAN shuts down the data VLAN.

BEFORE YOU BEGIN

Follow these guidelines to configure voice aware 802.1x voice security on the switch:

- You enable voice aware 802.1x security by entering the **reducible detect cause security-violation shutdown vlan** global configuration command. You disable voice aware 802.1x security by entering the **no** version of this command. This command applies to all 802.1x-configured ports in the switch.

Note If you do not include the **shutdown vlan** keywords, the entire port is shut down when it enters the error-disabled state.

- If you use the **errdisable recovery cause security-violation** global configuration command to configure error-disabled recovery, the port is automatically reenabled. If error-disabled recovery is not configured for the port, you reenable it by using the **shutdown** and **no-shutdown** interface configuration commands.
- You can reenable individual VLANs by using the **clear errdisable interface** *interface-id* **vlan** [*vlan-list*] privileged EXEC command. If you do not specify a range, all VLANs on the port are enabled.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**errdisable detect cause security-violation shutdown vlan**	Shut down any VLAN on which a security violation error occurs. **Note** If the **shutdown vlan** keywords are not included, the entire port enters the error-disabled state and shuts down.
Step 3	**errdisable recovery cause security-violation**	(Optional) Enable automatic per-VLAN error recovery.
Step 4	**clear errdisable interface** *interface-id* **vlan** [*vlan-list*]	(Optional) Reenable individual VLANs that have been error disabled. • For *interface-id* specify the port on which to reenable individual VLANs. • (Optional) For *vlan-list* specify a list of VLANs to be reenabled. If *vlan-list* is not specified, all VLANs are reenabled.
Step 5	**shutdown** **no-shutdown**	(Optional) Reenable an error-disabled VLAN, and clear all error-disable indications.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show errdisable detect**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure the switch to shut down any VLAN on which a security violation error occurs:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

This example shows how to reenable all VLANs that were error disabled on port GigabitEthernet2/02/2:

```
Switch# clear errdisable interface GigabitEthernet2/0/2 vlan
```

You can verify your settings by entering the **show errdisable detect** privileged EXEC command.

Configuring 802.1x Violation Modes

You can configure an 802.1x port so that it shuts down, generates a syslog error, or discards packets from a new device when:

- a device connects to an 802.1x-enabled port.
- the maximum number of allowed devices have been authenticated on the port.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication dot1x** {**default**} *method1*	Create an 802.1x authentication method list. To create a default list to use when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the method to use in default situations. The default method list is automatically applied to all ports. For *method1*, enter the **group radius** keywords to apply the list of all RADIUS servers for authentication. **Note** Though other keywords are visible in the command-line help string, only the **group radius** keywords are supported.

	Command	Purpose
Step 4	**interface** *interface-id*	Specify the port connected to the client that is to be enabled for IEEE 802.1x authentication, and enter interface configuration mode.
Step 5	**switchport mode access**	Set the port to access mode.
Step 6	**authentication violation** {**shutdown** | **restrict** | **protect** | **replace**} or **dot1x violation-mode** {**shutdown** | **restrict** | **protect**}	Configure the violation mode. The keywords have these meanings: • **shutdown**–Error disable the port. • **restrict**–Generate a syslog error. • **protect**–Drop packets from any new device that sends traffic to the port. • **replace**–Tear down the old session and accept packets from any new device that sends traffic to the port.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show authentication**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure an 802.1x port to report a syslog error when an authentication error is detected:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default
Switch(config)# interface ethernet0/2
Switch(config-if)# switchport mode access
Switch(config-if) authentication violation restrict
Switch(config-if) end
```

Configuring 802.1x Authentication

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

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

This is the 802.1x AAA process:

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

7. The user disconnects from the port.
8. The switch sends a stop message to the accounting server.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication dot1x** {**default**} *method1*	Create an 802.1x authentication method list. To create a default list to use when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the method to use in default situations. The default method list is automatically applied to all ports. For *method1*, enter the **group radius** keywords to use the list of all RADIUS servers for authentication. **Note** Though other keywords are visible in the command-line help string, only the **group radius** keywords are supported.
Step 4	**dot1x system-auth-control**	Enable 802.1x authentication globally on the switch.
Step 5	**aaa authorization network** {**default**} **group radius**	(Optional) Configure the switch for user RADIUS authorization for all network-related service requests, such as VLAN assignment.
Step 6	**interface** *interface-id*	Specify the port connected to the client that is to be enabled for 802.1x authentication, and enter interface configuration mode.
Step 7	**authentication port-control auto**	Enable 802.1x authentication on the port.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show authentication**	Verify your entries.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure 802.1x authentication on a port:

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface ethernet0/2
Switch(config-if)# authentication port-control auto
Switch(config-if)# end
```

Configuring the Host Mode

Follow this procedure to allow a single host (client) or multiple hosts on an 802.1x-authorized port that has the **authentication port-control auto** interface configuration command set to **auto**.

Note This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to which multiple hosts are indirectly attached, and enter interface configuration mode.
Step 3	**authentication host-mode** [**multi-auth** | **multi-host** | **single-host**]	Set the authentication mode. The keywords have these meanings: • **multi-auth**–Allow multiple authenticated clients on the data VLAN. Each host is individually authenticated. **Note** The **multi-auth** keyword is only available with the **authentication host-mode** command. • **multi-host**–Allow multiple hosts on an 802.1x-authorized port after a single host has been authenticated. • **single-host**–Allow a single host (client) on an 802.1x-authorized port. Make sure that the **authentication port-control auto** interface configuration command set is set to **auto** for the specified interface.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show authentication** *interface-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note Although visible in the command-line interface help, the **authentication host-mode multi-domain** interface configuration command is not supported. Configuring this command on an interface puts it in the error-disabled state.

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

EXAMPLE

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

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication host-mode multi-host
```

Configuring 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. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**authentication periodic**	Enable periodic re-authentication of the client, which is disabled by default.
Step 4	**authentication timer** {{[**inactivity** | **reauthenticate**]} {**restart** *value*}} **or** **dot1x timeout reauth-period** *seconds*	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	**end**	Return to privileged EXEC mode.
Step 6	**show authentication** *interface-id*	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable periodic re-authentication, use the **no authentication periodic** interface configuration command. To return to the default number of seconds between re-authentication attempts, use the **no authentication timer reauthenticate** interface configuration command.

EXAMPLE

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

```
Switch(config-if)# authentication periodic
Switch(config-if)# authentication timer reauthenticate 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 **authentication periodic** interface configuration command. This step is optional. If you want to enable or disable periodic re-authentication, see the "Configuring Periodic Re-Authentication" section on page 2-36.

EXAMPLE

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

```
Switch(config-if)# authentication periodic
```

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 **authentication timer reauthenticate** interface configuration command controls the quiet period. 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. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**authentication timer reauthenticate** *value*	Time, in seconds, after which an automatic re-authentication attempt starts. The range is 1 to 65535 seconds; the default is 3600.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show authentication interface** *interface-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default quiet period, use the **no authentication timer reauthenticate** interface configuration command.

EXAMPLE

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

```
Switch(config-if)# authentication timer reauthenticate 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.

Follow this procedure to change the amount of time that the switch waits for client notification.This procedure is optional.

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.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**dot1x timeout tx-period** *seconds*	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	**end**	Return to privileged EXEC mode.
Step 5	**show authentication** *interface-id*	Verify your entries.
Step 6	**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** interface configuration command.

EXAMPLE

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 frame (assuming no response is received) to the client before restarting the authentication process. This procedure is optional.

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

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

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

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

EXAMPLE

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

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

Setting the Re-Authentication Number

You can also change the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. This procedure is optional.

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.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**dot1x max-reauth-req** *count*	Set the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 1 to 10; the default is 2.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show authentication** *interface-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

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

EXAMPLE

This example shows how to set 4 as the number of times that the switch restarts the authentication process before the port changes to the unauthorized state:

```
Switch(config-if)# dot1x max-reauth-req 4
```

Enabling MAC Move

MAC move allows an authenticated host to move from one port on the switch to another. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**authentication mac-move permit**	Enable the feature.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show run**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to globally enable MAC move on a switch:

```
Switch(config)# authentication mac-move permit
```

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-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```

Follow this procedure to configure 802.1x accounting after AAA is enabled on your switch. This procedure is optional.

BEFORE YOU BEGIN

You must configure the RADIUS server to perform accounting tasks, such as logging start, stop, and interim-update messages and time stamps.

Tip To allow your RADIUS server to perform accounting tasks, 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.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa accounting dot1x default start-stop group radius**	Enable 802.1x accounting using the list of all RADIUS servers.
Step 3	**aaa accounting system default start-stop group radius**	(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.
Step 4	**end**	Return to privileged EXEc mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save 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.

EXAMPLE

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
```

Configuring a Guest VLAN

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 EAP request/identity frame. Clients that are 802.1x-capable but that fail authentication are not granted network access. The switch supports guest VLANs in single-host or multiple-hosts mode. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode access**	Set the port to access mode.
Step 4	**authentication port-control auto**	Enable 802.1x authentication on the port.
Step 5	**authentication event no-response action authorize vlan** *vlan-id*	Specify an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x guest VLAN. Voice VLANs are not supported.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show authentication** *interface-id*	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable and remove the guest VLAN, use the **no authentication event no-response action authorize vlan** *vlan-id* interface configuration command. The port returns to the unauthorized state.

EXAMPLE

This example shows how to enable VLAN 2 as an 802.1x guest VLAN:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# authentication event no-response action authorize vlan 2
```

This example shows how to set 3 as the quiet period 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)# authentication timer reauthenticate 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# authentication event no-response action authorize vlan 2
```

Configuring a Restricted VLAN

When you configure a restricted VLAN on a switch, clients that are 802.1x-compliant are moved into the restricted VLAN when the authentication server does not receive a valid username and password. The switch supports restricted VLANs only in single-host mode. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode access**	Set the port to access mode.
Step 4	**authentication port-control auto**	Enable 802.1x authentication on the port.
Step 5	**authentication event fail action authorize** *vlan-id*	Specify an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN. Voice VLANs are not supported.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show authentication** *interface-id*	(Optional) Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable and remove the restricted VLAN, use the **no authentication event fail** interface configuration command. The port returns to the unauthorized state.

EXAMPLE

This example shows how to enable *VLAN 2* as an 802.1x restricted VLAN:

```
Switch(config-if)# authentication event fail action authorize vlan 2
```

Configuring the Number of Authentication Attempts

You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the **authentication event fail retry** *retry count* interface configuration command. The range of allowable authentication attempts is 1 to 5. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode access**	Set the port to access mode.
Step 4	**authentication port-control auto**	Enable 802.1x authentication on the port.
Step 5	**authentication event fail action authorize vlan** *vlan-id*	Specify an active VLAN as an 802.1x restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1x restricted VLAN. Voice VLANs are not supported.
Step 6	**authentication event retry** *retry count*	Specify the number of authentication attempts to allow before a port moves to the restricted VLAN. The range is 1 to 5.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show authentication** *interface-id*	(Optional) Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the default value, use the **no authentication event fail action authorize vlan** *vlan-id* **retry** interface configuration command.

EXAMPLE

This example shows how to set 4 as the number of authentication attempts allowed before the port moves to the restricted VLAN 2:

```
Switch(config-if)# authentication event fail action authorize vlan 2 retry 4
```

Configuring the Inaccessible Authentication Bypass Feature

You can configure the inaccessible bypass feature, also referred to as critical authentication or the AAA fail policy. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server dead-criteria time** *time* **tries** *tries*	(Optional) Set the conditions that are used to decide when a RADIUS server is considered unavailable or *dead*. The range for *time* is from 1 to 120 seconds. The switch dynamically determines the default *time* value that is 10 to 60 seconds. The range for *tries* is from 1 to 100. The switch dynamically determines the default *tries* parameter that is 10 to 100.
Step 3	**radius-server deadtime** *minutes*	(Optional) Set the number of minutes that a RADIUS server is not sent requests. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.

	Command	Purpose
Step 4	**radius-server host** *ip-address* **[acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]	(Optional) Configure the RADIUS server parameters by using these keywords: • **acct-port** *udp-port*—Specify the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646. • **auth-port** *udp-port*—Specify the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645. **Note** You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values. • **test username** *name*—Enable automated testing of the RADIUS server status, and specify the username to be used. • **idle-time** *time*—Set the interval of time in minutes after which the switch sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour). • **ignore-acct-port**—Disable testing on the RADIUS-server accounting port. • **ignore-auth-port**—Disable testing on the RADIUS-server authentication port. • **key** *string*—Specify the authentication and encryption key for all RADIUS communication between the switch and the RADIUS daemon. **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. You can also configure the authentication and encryption key by using the **radius-server key** {**0** *string* | **7** *string* | *string*} global configuration command.
Step 5	**dot1x critical eapol**	(Optional) Specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.

	Command	Purpose
Step 6	**authentication critical recovery delay** *milliseconds*	(Optional) Set the recovery delay period during which the switch waits to re-initialize a critical port when a RADIUS server that was unavailable becomes available. The range is from 1 to 10000 milliseconds. The default is 1000 milliseconds (a port can be re-initialized every second).
Step 7	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 8	**authentication event server dead action authorize vlan** *vlan-id*	Enable the inaccessible authentication bypass feature.
Step 9	**authentication event server alive action reinitialize**	Reinitialize all clients on the port.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**show authentication interface** *interface-id*	(Optional) Verify your entries.
Step 12	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To return to the RADIUS server default settings, use the **no radius-server dead-criteria**, the **no radius-server deadtime**, and the **no radius-server host** global configuration commands. To return to the default settings of inaccessible authentication bypass, use the **no dot1x critical eapol** and **no authentication critical recovery delay** global configuration commands. To disable inaccessible authentication bypass, use the **no authentication event server alive action reinitialize** interface configuration command.

EXAMPLE

This example shows how to configure the inaccessible authentication bypass feature:

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
Switch(config)# dot1x critical eapol
Switch(config)# authentication critical recovery delay 2000
Switch(config)# interface gigabitethernet0/2
Switch(config)# radius-server deadtime 60
Switch(config-if)# interface gigabitethernet2/0/1
Switch(config-if)# authentication event server dead action authorize vlan 20
Switch(config-if)# authentication event server alive action reinitialize
Switch(config-if)# end
```

Configuring 802.1x Authentication with Wake-on-LAN

This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**authentication control-direction** {**both** | **in**}	Enable 802.1x authentication with Wake-on-LAN (WoL) on the port, and use these keywords to configure the port as bidirectional or unidirectional. • **both**—Sets the port as bidirectional. The port cannot receive packets from or send packets to the host. By default, the port is bidirectional. • **in**—Sets the port as unidirectional. The port can send packets to the host but cannot receive packets from the host.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show authentication interface** *interface-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable 802.1x authentication with WoL, use the **no authentication control-direction** interface configuration command.

EXAMPLE

This example shows how to enable 802.1x authentication with Wake-on-LAN (WoL) and set the port as bidirectional:

```
Switch(config-if)# authentication control-direction both
```

Configuring MAC Authentication Bypass

This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode. For the supported port types, see the "Guidelines and Limitations" section on page 2-24.

	Command	Purpose
Step 3	**authentication port-control auto**	Enable 802.1x authentication on the port.
Step 4	**mab** [**eap**]	Enable MAC authentication bypass (MAB). (Optional) Use the **eap** keyword to configure the switch to use EAP for authorization.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show authentication** *interface-id*	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable MAC authentication bypass, use the **no mab** interface configuration command.

EXAMPLE

This example shows how to enable MAC authentication bypass:

```
Switch(config-if)# mab
```

Configuring 802.1x User Distribution

Follow this procedure to configure a VLAN group and to map a VLAN to it.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**vlan group** *vlan-group-name* **vlan-list** *vlan-list*	Configure a VLAN group, and map a single VLAN or a range of VLANs to it.
Step 2	**show vlan group all** *vlan-group-name*	Verify the configuration.
Step 3	**no vlan group** *vlan-group-name* **vlan-list** *vlan-list*	Clear the VLAN group configuration or elements of the VLAN group configuration.

EXAMPLE

This example shows how to configure the VLAN groups, map the VLANs to the groups, and verify the VLAN group configurations and mapping to the specified VLANs:

```
switch(config)# vlan group eng-dept vlan-list 10
end
switch# show vlan group group-name eng-dept
Group Name                      Vlans Mapped
-------------                   --------------
eng-dept                        10

switch# show vlan-group all
Group Name                      Vlans Mapped
```

```
-------------                    --------------
eng-dept                         10
hr-dept                          20
```

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

```
switch(config)# vlan group eng-dept vlan-list 30
end
switch# show vlan group eng-dept
Group Name                       Vlans Mapped
-------------                    --------------
eng-dept                         10,30
```

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

```
switch(config)# no vlan group eng-dept vlan-list 10
```

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

```
switch(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.
end
switch# show vlan group group-name eng-dept
```

This example shows how to clear all the VLAN groups:

```
switch(config)# no vlan group end-dept vlan-list all
end
switch# show vlan-group all
```

Configuring NAC Layer 2 IEEE 802.1x Validation

You can configure NAC Layer 2 802.1x validation, which is also referred to as 802.1x authentication with a RADIUS server. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**authentication event no-response action authorize vlan** *vlan-id*	Specify an active VLAN as an 802.1x guest VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, or a voice VLAN as an 802.1x guest VLAN. Voice VLANs are not supported.

	Command	Purpose
Step 4	**authentication periodic**	Enable periodic re-authentication of the client, which is disabled by default.
Step 5	**authentication timer reauthenticate** *value*	Set the number of seconds between re-authentication attempts. The keyword has this meaning: • *value*—Sets the number of seconds from 1 to 65535. The default is 3600 seconds. This command affects the behavior of the switch only if periodic re-authentication is enabled.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show authentication** *interface-id*	Verify your 802.1x authentication configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure NAC Layer 2 802.1x validation:

```
Switch# configure terminal
Switch(config)# interface fastethernetethernet0/3
Switch(config-if)# authentication periodic
```

Resetting the 802.1x Authentication Configuration to the Default Values

This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and specify the port to be configured.
Step 3	**dot1x default**	Reset the configurable 802.1x parameters to the default values.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show dot1x interface** *interface-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

```
Switch(config)# interface fastethernetethernet0/3
Switch(config-if)# dot1x default
```

```
Switch(config-if)# end
```

Disabling 802.1x Authentication on the Port

You can disable 802.1x authentication on the port by using the **no dot1x pae** interface configuration command. This procedure is optional.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**no dot1x pae**	Disable 802.1x authentication on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show authentication** *interface-id*	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To configure the port as an 802.1x port access entity (PAE) authenticator, which enables IEEE 802.1x on the port but does not allow connected clients to be authorized, use the **dot1x pae authenticator** interface configuration command.

EXAMPLE

This example shows how to disable 802.1x authentication on the port:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# no dot1x pae authenticator
```

Configuring an Authenticator and a Supplicant Switch with NEAT

Configuring this feature requires that one switch outside a wiring closet is configured as a supplicant and is connected to an authenticator switch.

For overview information, see the "802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)" section on page 2-23.

Note The *cisco-av-pairs* must be configured as *device-traffic-class=switch* on the ACS, which sets the interface as a trunk after the supplicant is successfully authenticated.

Configuring the Authenticator

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cisp enable**	Enable CISP.
Step 3	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 4	**switchport mode access**	Set the port mode to **access**.
Step 5	**authentication port-control auto**	Set the port-authentication mode to auto.
Step 6	**dot1x pae authenticator**	Configure the interface as a port access entity (PAE) authenticator.
Step 7	**spanning-tree portfast trunk**	Enable Port Fast on an access port connected to a single workstation or server.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show running-config interface** *interface-id*	Verify your configuration.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure a switch as an 802.1x authenticator:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# spanning-tree portfast trunk
```

Configuring the Supplicant

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cisp enable**	Enable CISP.
Step 3	**dot1x credentials** *profile*	Create 802.1x credentials profile. This must be attached to the port that is configured as supplicant.
Step 4	**username** *suppswitch*	Create a username.
Step 5	**password** *password*	Create a password for the new username.
Step 6	**dot1x supplicant force-multicast**	Force the switch to send *only* multicast EAPOL packets when it receives either unicast or multicast packets. This also allows NEAT to work on the supplicant switch in all host modes.
Step 7	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 8	**switchport trunk encapsulation dot1q**	Set the port to trunk mode.
Step 9	**switchport mode trunk**	Configure the interface as a VLAN trunk port.
Step 10	**dot1x pae supplicant**	Configure the interface as a port access entity (PAE) supplicant.
Step 11	**dot1x credentials** *profile-name*	Attach the 802.1x credentials profile to the interface.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**show running-config interface** *interface-id*	Verify your configuration.
Step 14	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure a switch as a supplicant:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# dot1x credentials test
Switch(config)# username suppswitch
Switch(config)# password myswitch
Switch(config)# dot1x supplicant force-multicast
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1x pae supplicant
Switch(config-if)# dot1x credentials test
Switch(config-if)# end
```

Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs

In addition to configuring 802.1x authentication on the switch, you need to configure the ACS. For more information, see the Cisco Secure ACS configuration guides.

Note You must configure a downloadable ACL on the ACS before downloading it to the switch.

After authentication on the port, you can use the **show ip access-list** privileged EXEC command to display the downloaded ACLs on the port.

Configuring Downloadable ACLs

The policies take effect after client authentication and the client IP address addition to the IP device tracking table. The switch then applies the downloadable ACL to the port.

BEFORE YOU BEGIN

Configure an ACL. See Chapter 6, "Configuring Network Security with ACLs" or Chapter 7, "Configuring IPv6 ACLs."

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip device tracking**	Configure the ip device tracking table.
Step 3	**aaa new-model**	Enable AAA.
Step 4	**aaa authorization network default group radius**	Set the authorization method to local. To remove the authorization method, use the **no aaa authorization network default group radius** command.
Step 5	**radius-server vsa send authentication**	Configure the network access server (NAS) to recognize and use only authentication vendor-specific attributes (VSAs).
Step 6	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 7	**ip access-group** *acl-id* **in**	Configure the default ACL on the port in the input direction. **Note** The *acl-id* is an access list name or number.
Step 8	**show running-config interface** *interface-id*	Verify your configuration.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

```
Switch(config)# ip device tracking
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group default_acl in
```

Configuring a Downloadable Policy

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**access-list** *access-list-number* **deny source** *source-wildcard* **log**	Defines the default port ACL by using a source address and wildcard. The access-list-number is a decimal number from 1 to 99 or 1300 to 1999. Enter **deny** or **permit** to specify whether to deny or permit access if conditions are matched. The *source* is the source address of the network or host that sends a packet, such as this: • The 32-bit quantity in dotted-decimal format. • The keyword any as an abbreviation for source and source-wildcard value of 0.0.0.0 255.255.255.255. You do not need to enter a source-wildcard value. • The keyword host as an abbreviation for source and source-wildcard of source 0.0.0.0. (Optional) Applies the source-wildcard wildcard bits to the source. (Optional) Enters log to cause an informational logging message about the packet that matches the entry to be sent to the console.
Step 3	**interface** *interface-id*	Enter interface configuration mode.
Step 4	**ip access-group** *acl-id* **in**	Configure the default ACL on the port in the input direction. **Note** The *acl-id* is an access list name or number.
Step 5	**exit**	Returns to global configuration mode.
Step 6	**aaa new-model**	Enables AAA.
Step 7	**aaa authorization network default group radius**	Sets the authorization method to local. To remove the authorization method, use the **no aaa authorization network default group radius** command.
Step 8	**ip device tracking**	Enables the IP device tracking table. To disable the IP device tracking table, use the **no ip device tracking** global configuration command.

	Command	Purpose
Step 9	**ip device tracking probe count** *count*	(Optional) Configures the IP device tracking table: • **count** *count*–Sets the number of times that the switch sends the ARP probe. The range is from 1 to 5. The default is 3.
Step 10	**radius-server vsa send authentication**	Configures the network access server to recognize and use vendor-specific attributes (VSAs). **Note** The downloadable ACL must be operational.
Step 11	**end**	Returns to privileged EXEC mode.
Step 12	**show ip device tracking all**	Displays information about the entries in the IP device tracking table.
Step 13	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

EXAMPLE

This example shows how to configure a switch for a downloadable policy:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

Configuring VLAN ID-based MAC Authentication

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mab request format attribute 32 vlan access-vlan**	Enable VLAN ID-based MAC authentication.
Step 3	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

There is no show command to confirm the status of VLAN ID-based MAC authentication. You can use the **debug radius accounting** privileged EXEC command to confirm the RADIUS attribute 32. For more information about this command, see the Cisco IOS Debug Command Reference.

EXAMPLE

This example shows how to globally enable VLAN ID-based MAC authentication on a switch:

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# mab request format attribute 32 vlan access-vlan
Switch(config-if)# exit
```

Configuring Flexible Authentication Ordering

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**authentication order** [**dot1x** | **mab**] | {**webauth**}	(Optional) Set the order of authentication methods used on a port.
Step 4	**authentication priority** [**dot1x** | **mab**] | {**webauth**}	(Optional) Add an authentication method to the port-priority list.
Step 5	**show authentication**	(Optional) Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure a port attempt 802.1x authentication first, followed by web authentication as fallback method:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config)# authentication order dot1x webauth
```

Configuring Open1x

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**authentication control-direction** {**both** | **in**}	(Optional) Configure the port control as unidirectional or bidirectional.
Step 4	**authentication fallback** *name*	(Optional) Configure a port to use web authentication as a fallback method for clients that do not support 802.1x authentication.
Step 5	**authentication host-mode** [**multi-auth** | **multi-host** | **single-host**]	(Optional) Set the authorization manager mode on a port. **Note** Although visible in the command-line interface help, the **authentication host-mode multi-domain** interface configuration command is not supported. Configuring this command on an interface causes the interface to go into the error-disabled state.
Step 6	**authentication open**	(Optional) Enable or disable open access on a port.
Step 7	**authentication order** [**dot1x** | **mab**] | {**webauth**}	(Optional) Set the order of authentication methods used on a port.
Step 8	**authentication periodic**	(Optional) Enable or disable re-authentication on a port.
Step 9	**authentication port-control** {**auto** | **force-authorized** | **force-un authorized**}	(Optional) Enable manual control of the port authorization state.
Step 10	**show authentication**	(Optional) Verify your entries.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure Open1x on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config)# authentication control-direction both
Switch(config)# au ten tic at ion fallback profile1
Switch(config)# authentication host-mode multi-auth
Switch(config)# authentication open
Switch(config)# authentication order dot1x webauth
Switch(config)# authentication periodic
Switch(config)# authentication port-control auto
```

Verifying Configuration

Command	Purpose
show dot1x all statistics	Display 802.1x statistics for all ports.
show dot1x statistics interface *interface-id*	Display 802.1x statistics for a specific port.
show dot1x all or **show authentication method dotx**	Display the 802.1x administrative and operational status for the switch.
show dot1x interface *interface-id* or **show authentication interface** *interface-id*	Display the 802.1x administrative and operational status for a specific port.

Related Documents

- Cisco IOS Master Command List, All Releases
- Cisco IOS Debug Command Reference
- Cisco IOS Security Command Reference
- *Cisco Connected Grid Switches Security Software Configuration Guide*
  - "Configuring the Switch to Use Vendor-Specific RADIUS Attributes" section within the "Configuring Switch-Based Authentication" chapter
  - "Configuring Network Security with ACLs"