Configuring IEEE 802.1X Port-Based Authentication

This chapter describes how to configure IEEE 802.1X port-based authentication in Cisco IOS Software Release 12.2SX to prevent unauthorized devices (clients) from gaining access to the network.

Note
For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Software Releases 12.2SX Command References at this URL:

This chapter consists of these sections:
- Understanding 802.1X Port-Based Authentication, page 52-1
- Configuring 802.1X Port-Based Authentication, page 52-18
- Displaying 802.1X Status, page 52-41

Understanding 802.1X Port-Based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

These sections describe the role of 802.1X port-based authentication as a part of a system of authentication, authorization, and accounting (AAA):
- Device Roles, page 52-2
- Authentication Process, page 52-3
- Authentication Initiation and Message Exchange, page 52-5
- Ports in Authorized and Unauthorized States, page 52-7
- 802.1X Host Mode, page 52-8
Device Roles

With 802.1X port-based authentication, the devices in the network have specific roles as shown in Figure 52-1.

The specific roles shown in Figure 52-1 are as follows:

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

  **Note** To resolve Windows XP network connectivity and 802.1X port-based authentication issues, read the Microsoft Knowledge Base article at this URL:
  http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

- **Authentication server**—Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. The Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported...
authentication server; it is available in Cisco Secure Access Control Server, version 3.0. RADIUS uses a client-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- **Switch** (also called the authenticator and back-end authenticator)—With Release 12.2(33)SXH and later releases, 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 reencapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the 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 receives 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 user-specified critical VLAN.

**Note**  
Inaccessible authentication bypass is also referred to as critical authentication or the AAA fail policy.
Figure 52-2 shows the authentication process.

The switch reauthenticates a client when one of these situations occurs:

- Periodic reauthentication is enabled, and the reauthentication timer expires.
  
  You can configure the reauthentication 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 reauthentication occurs.
Chapter 52      Configuring IEEE 802.1X Port-Based Authentication

Understanding 802.1X Port-Based Authentication

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during reauthentication. 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 reauthentication. When the ReAuthenticate action is set (the attribute value is RADIUS-Request), the session is not affected during reauthentication.

- You manually reauthenticate the client by entering the `dot1x re-authenticate interface type slot/port` privileged EXEC command.

Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the `dot1x port-control auto` interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. The switch then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). When the client receives the frame, it responds with an EAP-response/identity frame.

If the client does not receive an EAP-request/identity frame from the switch during bootup, 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 transmits 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 52-7.

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 port becomes authorized. If the authentication fails, authentication can be retried, the port might be assigned to a VLAN that provides limited services, or network access is not granted. For more information, see the “Ports in Authorized and Unauthorized States” section on page 52-7.
The specific exchange of EAP frames depends on the authentication method being used. Figure 52-3 shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

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.
Ports in Authorized and Unauthorized States

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

If a client that does not support 802.1X authentication 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 protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

You control the port authorization state by using the `dot1x port-control` interface configuration command and these keywords:

- **force-authorized**—Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. This is the default setting.

- **force-unauthorized**—Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface.

- **auto**—Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client’s MAC address.
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

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

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

802.1X Host Mode

You can configure an 802.1X port for single-host or for multiple-hosts mode. In single-host mode (see Figure 52-1 on page 52-2), only one client can be connected to the 802.1X-enabled 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 52-5 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 (reauthentication 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 authentication to authenticate the port and port security to manage network access for all MAC addresses, including that of the client.

Using 802.1X Authentication with DHCP Snooping

With Release 12.2(33)SXH and later releases, when the Dynamic Host Configuration Protocol (DHCP) snooping option-82 with data insertion feature is enabled, the switch can insert a client’s 802.1X authenticated user identity information into the DHCP discovery process, allowing the DHCP server to
assign IP addresses from different IP address pools to different classes of end users. This feature allows you to secure the IP addresses given to the end users for accounting purposes and to grant services based on Layer 3 criteria.

After a successful 802.1X authentication between a supplicant and the RADIUS server, the switch puts the port in the forwarding state and stores the attributes that it receives from the RADIUS server. While performing DHCP snooping, the switch acts as a DHCP relay agent, receiving DHCP messages and regenerating those messages for transmission on another interface. When a client, after 802.1X authentication, sends a DHCP discovery message, the switch receives the packet. The switch adds to the packet a RADIUS attributes suboption section containing the stored RADIUS attributes of the client. The switch then submits the discovery broadcast again. The DHCP server receives the modified DHCP discovery packet and, if configured to do so, use the authenticated user identity information when creating the IP address lease. The mapping of user-to-IP address can be on a one-to-one, one-to-many, or many-to-many basis. The one-to-many mapping allows the same user to authenticate through the 802.1X hosts on multiple ports.

The switch will automatically insert the authenticated user identity information when 802.1X authentication and DHCP snooping option-82 with data insertion features are enabled. To configure DHCP snooping option-82 with data insertion, see the “DHCP Snooping Option-82 Data Insertion” section on page 46-3.

For information about the data inserted in the RADIUS attributes suboption, see RFC 4014, “Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option.”

**802.1X Accounting**

The IEEE 802.1X standard defines how users are authorized and authenticated for network access but does not keep track of network usage. IEEE 802.1X accounting is disabled by default. With Release 12.2(33)SXH and later releases, you can enable 802.1X accounting to monitor this activity on 802.1X-enabled ports:

- User successfully authenticates.
- User logs off.
- Link-down occurs.
- Reauthentication successfully occurs.
- Reauthentication fails.

The switch does not log IEEE 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 in the Acct-Input-Octets or the Acct-Output-Octets attributes of a RADIUS packet.) AV pairs are automatically sent by a switch that is configured for 802.1X accounting. Three types of RADIUS accounting packets are sent by a switch:

- START—Sent when a new user session starts.
- INTERIM—Sent during an existing session for updates.
- STOP—Sent when a session terminates.
Table 52-1 lists the AV pairs and indicates when they are sent by the switch.

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

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

You can view the AV pairs that are being sent by the switch by entering the `debug radius accounting` privileged EXEC command. For more information about this command, see the *Cisco IOS Debug Command Reference, Release 12.2* at this URL:


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

Using 802.1X Authentication with VLAN Assignment

After successful 802.1X authentication of a port, the RADIUS server sends the VLAN assignment to configure the port. The RADIUS server database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the client connected to the port. You can use this feature to limit network access for certain users.
When configured on the switch and the RADIUS server, 802.1X authentication with VLAN assignment has these characteristics:

- If no VLAN is supplied by the RADIUS server or if 802.1X authentication is disabled, the port is configured in its access VLAN after successful authentication. 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 authentication 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, or an attempted assignment to a voice VLAN ID.

- If 802.1X authentication is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.

- If the multiple-hosts mode is enabled on an 802.1X port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.

- If 802.1X authentication and port security are enabled on a port, the port is placed in the RADIUS server-assigned VLAN.

- 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, force-unauthorized, unauthorized, or 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 authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).

To configure VLAN assignment you need to perform these tasks:

---

**Step 1**
Enable AAA authorization by using the `network` keyword to allow interface configuration from the RADIUS server.

**Step 2**
Enable 802.1X authentication. (The VLAN assignment feature is automatically enabled when you configure 802.1X authentication on an access port).

**Step 3**
Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the switch:

- [64] Tunnel-Type = VLAN
- [65] Tunnel-Medium-Type = 802
- [81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

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

With Release 12.2(33)SXH and later releases, 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 Windows 98 systems, 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.

In addition, 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 will not change to the guest VLAN state. The EAPOL packet history is cleared if the interface link status goes down.

Use the `dot1x guest-vlan supplicant` global configuration command to allow an interface to change to the guest VLAN state regardless of the EAPOL packet history. That is, a host that is not 802.1X-capable will be assigned to the guest VLAN even if a previous host on that interface was 802.1X-capable.

Notes

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 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.

When operating as an 802.1X guest VLAN, a port functions in multiple-hosts mode regardless of the configured host mode of the port.

You can configure any active VLAN except an RSPAN VLAN, a private primary PVLAN, or a voice VLAN as an 802.1X guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

The switch supports MAC authentication bypass in Release 12.2(33)SXH and later releases. 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 “Using 802.1X Authentication with MAC Authentication Bypass” section on page 52-17.

For more information, see the “Configuring a Guest VLAN” section on page 52-32.

Using 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.
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 port remains in the spanning-tree blocking state. With this feature, you can configure the 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 reauthentication attempt. A port in the restricted VLAN tries to reauthenticate at configured intervals (the default is 60 seconds). If reauthentication fails, the port remains in the restricted VLAN. If reauthentication is successful, the port moves either to the configured VLAN or to a VLAN sent by the RADIUS server. You can disable reauthentication. If you do this, the only way to restart the authentication process is for the port to receive a link down or EAP logoff event. We recommend that you keep reauthentication 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.

When operating as an 802.1X restricted VLAN, a port functions in single-host mode regardless of the configured host mode of the port.

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 52-33.

**Using 802.1X Authentication with Inaccessible Authentication Bypass**

With Release 12.2(33)SXH and later releases, when the switch cannot reach the configured RADIUS servers and hosts cannot be authenticated, you can configure the switch to allow network access to the hosts connected to critical ports. A critical port is enabled for the inaccessible authentication bypass feature, also referred to as critical authentication or the AAA fail policy.

When this feature is enabled, the switch checks the status of the configured RADIUS servers whenever the switch tries to authenticate a host connected to a critical port. 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.
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 user-specified critical VLAN.
- If the port is already authorized and reauthentication 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 exchanges times out, and the switch puts the critical port in the critical-authentication state during the next authentication attempt.

When a RADIUS server that can authenticate the host is available, all critical ports in the critical-authentication state are automatically reauthenticated.

Inaccessible authentication bypass interacts with these features:

- **Guest VLAN**—Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on 802.1x 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 user-specified critical 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.
- **Voice VLAN**—Inaccessible authentication bypass is compatible with voice VLAN, but the RADIUS-configured or user-specified access VLAN and the voice VLAN must be different.
- **Remote Switched Port Analyzer (RSPAN)**—Do not configure an RSPAN VLAN as the RADIUS-configured or user-specified access VLAN for inaccessible authentication bypass.
Using 802.1X Authentication with Voice VLAN Ports

A Multi-VLAN Access Port (MVAP) is a port that belong to two VLANs. A voice VLAN port is an MVAP that allows separating a port’s voice traffic and data traffic on different VLANs. A voice VLAN port is associated with two VLAN identifiers:

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

In releases earlier than Release 12.2(33)SXH, a switch in single-host mode accepted traffic from a single host, and voice traffic was not allowed. In multiple-hosts mode, the switch did not accept voice traffic until the client was authenticated on the primary VLAN, which makes the IP phone inoperable until the user logged in.

With Release 12.2(33)SXH and later releases, the IP phone uses the VVID for its voice traffic, regardless of the authorization state of the port. This allows the phone to work independently of 802.1X authentication.

In single-host mode, only the IP phone is allowed on the voice VLAN. In multiple-hosts mode, additional clients can send traffic on the voice VLAN after a supplicant is authenticated on the PVID. When multiple-hosts mode is enabled, the supplicant authentication affects both the PVID and the VVID.

In order to recognize an IP phone, the switch will allow CDP traffic on a port regardless of the authorization state of the port. A voice VLAN port becomes active when there is a link, and the device MAC address appears after the first CDP message from the IP phone. Cisco IP phones do not relay CDP messages from other devices. As a result, if several IP phones are connected in series, the switch recognizes only the one directly connected to it. When 802.1X authentication is enabled on a voice VLAN port, the switch drops packets from unrecognized IP phones more than one hop away.

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

---

**Note**

If you enable 802.1X authentication on an access port on which a voice VLAN is configured and to which a Cisco IP Phone is connected, the Cisco IP phone loses connectivity to the switch for up to 30 seconds.

For voice VLAN configuration information, see Chapter 12, “Configuring Cisco IP Phone Support.”

---

Using 802.1X Authentication with Port Security

With Release 12.2(33)SXH and later releases, 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 authentication on a port, 802.1X authentication 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 authentication 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.

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. For more information, see the “Configuring the Port Security Violation Mode on a Port” section on page 54-6.

- 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 reauthenticate the 802.1X client by using the `dot1x re-authenticate interface type slot/port` privileged EXEC 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.

- Port security and a voice VLAN can be configured simultaneously on an 802.1X port that is in either single-host or multiple-hosts mode. Port security applies to both the voice VLAN identifier (VVID) and the port VLAN identifier (PVID).

For more information about enabling port security on your switch, see the “Configuring Port Security” section on page 54-4.

### Using 802.1X Authentication with Wake-on-LAN

With Release 12.2(33)SXH and later releases, the 802.1X authentication with 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 `dot1x 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 `dot1x 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.

### Using 802.1X Authentication with MAC Authentication Bypass

With Release 12.2(33)SXH and later releases, you can configure the switch to authorize clients based on the client MAC address (see Figure 52-4 on page 52-7) 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 reauthentication occurs, the switch uses 802.1X authentication as the preferred reauthentication 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 reauthenticated. The reauthentication process is the same as that for clients that were authenticated with 802.1X. During reauthentication, the port remains in the previously assigned VLAN. If reauthentication is successful, the switch keeps the port in the same VLAN. If reauthentication fails, the switch assigns the port to the guest VLAN, if one is configured.

If reauthentication 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 reauthentication. If MAC authentication bypass is enabled and the 802.1X authentication times out, the switch uses the MAC authentication bypass feature to initiate reauthorization. For more information about these AV pairs, see RFC 3580, “IEEE 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.
Configuring 802.1X Port-Based Authentication

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

- Default 802.1X Port-Based Authentication Configuration, page 52-19
- 802.1X Authentication Feature Configuration Guidelines, page 52-20
- Enabling 802.1X Authentication, page 52-22
- Configuring Switch-to-RADIUS-Server Communication, page 52-25
- Enabling Multiple Hosts, page 52-26
- Enabling Periodic Reauthentication, page 52-26
- Manually Reauthenticating the Client Connected to a Port, page 52-27
- Initializing Authentication for the Client Connected to a Port, page 52-28
- Removing 802.1X Client Information, page 52-28
- Changing 802.1X Timeouts, page 52-29
- Setting the Switch-to-Client Frame Retransmission Number, page 52-30
- Setting the Reauthentication Number, page 52-31
- Configuring IEEE 802.1X Accounting, page 52-32
- Configuring a Guest VLAN, page 52-32

Using Network Admission Control Layer 2 IEEE 802.1X Validation

Release 12.2(33)SXH and later supports Network Admission Control (NAC) Layer 2 IEEE 802.1X validation, which checks the antivirus condition or posture of endpoint systems or clients before granting the devices network access. NAC Layer 2 IEEE 802.1X validation performs policy enforcement by assigning the authenticated port into a specified VLAN, which provides segmentation and quarantine of poorly postured hosts at Layer 2.

Configuring NAC Layer 2 IEEE 802.1X validation is similar to configuring 802.1X port-based authentication except that you must configure a posture token on the RADIUS server. You can view the NAC posture token, which shows the posture of the client, by using the show dot1x privileged EXEC command. For information about configuring NAC Layer 2 IEEE 802.1X validation, see the “Configuring NAC Layer 2 IEEE 802.1X Validation” section on page 52-39.

For more information about NAC, see the Network Admission Control Software Configuration Guide.
Default 802.1X Port-Based Authentication Configuration

Table 52-2 shows the default 802.1X configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 802.1X enable state</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Per-port 802.1X enable state</td>
<td>Disabled (force-authorized). The port sends and receives normal traffic without 802.1X-based authentication of the client.</td>
</tr>
<tr>
<td>AAA</td>
<td>Disabled.</td>
</tr>
<tr>
<td>RADIUS server</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>None specified.</td>
</tr>
<tr>
<td>UDP authentication port</td>
<td>1812.</td>
</tr>
<tr>
<td>Key</td>
<td>None specified.</td>
</tr>
<tr>
<td>Host mode</td>
<td>Single-host mode.</td>
</tr>
<tr>
<td>Control direction</td>
<td>Bidirectional control.</td>
</tr>
<tr>
<td>Periodic reauthentication</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Number of seconds between reauthentication attempts</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Reauthentication number</td>
<td>2 times (number of times that the switch restarts the authentication process before the port changes to the unauthorized state).</td>
</tr>
<tr>
<td>Quiet period</td>
<td>60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client)</td>
</tr>
<tr>
<td>Retransmission time</td>
<td>30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before retransmitting the request)</td>
</tr>
<tr>
<td>Maximum retransmission number</td>
<td>2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process)</td>
</tr>
</tbody>
</table>

Table 52-2  Default 802.1X Configuration

- Configuring a Restricted VLAN, page 52-33
- Configuring the Inaccessible Authentication Bypass Feature, page 52-35
- Configuring 802.1X Authentication with WoL, page 52-37
- Configuring MAC Authentication Bypass, page 52-38
- Configuring NAC Layer 2 IEEE 802.1X Validation, page 52-39
- Disabling 802.1X Authentication on the Port, page 52-40
- Resetting the 802.1X Configuration to the Default Values, page 52-40
Configuring IEEE 802.1X Port-Based Authentication

### Table 52-2 Default 802.1X Configuration (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client timeout period</td>
<td>30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before retransmitting the request to the client)</td>
</tr>
<tr>
<td>Authentication server timeout period</td>
<td>30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before retransmitting the response to the server)</td>
</tr>
<tr>
<td>Inactivity timeout</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Inaccessible authentication bypass</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Restricted VLAN</td>
<td>None specified.</td>
</tr>
<tr>
<td>Authenticator (switch) mode</td>
<td>None specified.</td>
</tr>
<tr>
<td>MAC authentication bypass</td>
<td>Disabled.</td>
</tr>
</tbody>
</table>

802.1X Authentication Feature Configuration Guidelines

This section has configuration guidelines for these features:

- 802.1X Authentication
- VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass
- MAC Authentication Bypass

802.1X Authentication

These are the 802.1X authentication configuration guidelines:

- When 802.1X authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- If you try to change the mode of an 802.1X-enabled port (for example, from access to trunk), an error message appears, and the port mode is not changed.
- If the VLAN to which an 802.1X-enabled port is assigned changes, this change is transparent and does not affect the switch. For example, this change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after reauthentication.
  
If the VLAN to which an 802.1X port is assigned to shut down, disabled, or removed, the port becomes unauthorized. For example, the port is unauthorized after the access VLAN to which a port is assigned shuts down or is removed.

- The 802.1X protocol is supported on Layer 2 static-access ports, voice VLAN ports, and Layer 3 routed ports, but it is not supported on these port types:
  
- Trunk port—If you try to enable 802.1X authentication on a trunk port, an error message appears, and 802.1X authentication 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.
Chapter 52      Configuring IEEE 802.1X Port-Based Authentication

Configuring 802.1X Port-Based Authentication

– Dynamic ports—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X authentication on a dynamic port, an error message appears, and 802.1X authentication is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, an error message appears, and the port mode is not changed.

– Dynamic-access ports—If you try to enable 802.1X authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1X authentication 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 authentication on an EtherChannel port, an error message appears, and 802.1X authentication is not enabled.

Note

In software releases earlier than Release 12.2(33)SXH, if 802.1X authentication is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

– Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable 802.1X authentication on a port that is a SPAN or RSPAN destination port. However, 802.1X authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable 802.1X authentication on a SPAN or RSPAN source port.

Note

In software releases earlier than Release 12.2(33)SXH, 802.1X authentication is not supported on voice VLAN ports.

• Before globally enabling 802.1X authentication on a switch by entering the `dot1x system-auth-control` global configuration command, remove the EtherChannel configuration from the interfaces on which 802.1X authentication and EtherChannel are configured.

VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass

These are the configuration guidelines for VLAN assignment, guest VLAN, restricted VLAN, and inaccessible authentication bypass:

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

• The 802.1X authentication with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VMPS.

• You can configure any VLAN except an RSPAN VLAN, a private primary PVLAN, or a voice VLAN as an 802.1X guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

• After you configure a guest VLAN for an 802.1X port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the 802.1X authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. Decrease the settings for the 802.1X authentication process (`dot1x timeout quiet-period` and `dot1x timeout tx-period` interface configuration commands). The amount to decrease the settings depends on the connected 802.1X client type.
When configuring the inaccessible authentication bypass feature, follow these guidelines:

- The feature is supported on 802.1X port in single-host mode and multihosts mode.
- If the client is running Windows XP and the port to which the client is connected is in the critical-authentication state, Windows XP might report that the interface is not authenticated.
- If the Windows XP client is configured for DHCP and has an IP address from the DHCP server, receiving an EAP-Success message on a critical port might not reinitiate the DHCP configuration process.
- You can configure the inaccessible authentication bypass feature and the restricted VLAN on an 802.1X port. If the switch tries to reauthenticate a critical port in a restricted VLAN and all the RADIUS servers are unavailable, switch changes the port state to the critical authentication state and remains in the restricted VLAN.
- You can configure the inaccessible bypass feature and port security on the same port.

MAC Authentication Bypass

These are the MAC authentication bypass configuration guidelines:

- Unless otherwise stated, the MAC authentication bypass guidelines are the same as the 802.1X authentication guidelines. For more information, see the “802.1X Authentication” section on page 52-20.
- If you disable MAC authentication bypass from a port after the port has been authorized with its MAC address, the port state is not affected.
- If the port is in the unauthorized state and the client MAC address is not the authentication-server database, the port remains in the unauthorized state. However, if the client MAC address is added to the database, the switch can use MAC authentication bypass to reauthorize the port.
- If the port is in the authorized state, the port remains in this state until reauthorization occurs.
- To use MAC authentication bypass on a routed port, make sure that MAC address learning is enabled on the port.
- In Release 12.2(33)SXH and later, you can configure a timeout period for hosts that are connected by MAC authentication bypass but are inactive. The range is 1–65535 seconds. You must enable port security before configuring a timeout value. For more information, see the “Configuring Port Security” section on page 54-4.

Enabling 802.1X Authentication

To enable 802.1X port-based authentication, you must enable AAA and specify the authentication method list.

A method list describes the sequence and authentication methods to be queried to authenticate a user. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.
To allow VLAN assignment, you must enable AAA authorization to configure the switch for all network-related service requests.

The 802.1X AAA process is as follows:

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. Reauthentication is performed, as necessary.
6. The switch sends an interim accounting update to the accounting server that is based on the result of reauthentication.
7. The user disconnects from the port.
8. The switch sends a stop message to the accounting server.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Router(config)# aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# no aaa new-model</td>
<td>Disables AAA.</td>
</tr>
<tr>
<td>2</td>
<td>Router(config)# aaa authentication dot1x (\text{default} ) method1 [method2...)]</td>
<td>Creates an 802.1X port-based authentication method list. To create a default list that is used when a named list is not specified in the authentication command, use the default keyword followed by the method that is to be used 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. Though other keywords are visible in the command-line help string, only the group radius keywords are supported.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# no aaa authentication dot1x (\text{default} ) list_name</td>
<td>Clears the configured method list.</td>
</tr>
<tr>
<td>3</td>
<td>Router(config)# dot1x system-auth-control</td>
<td>Globally enables 802.1X port-based authentication.</td>
</tr>
<tr>
<td></td>
<td>Router(config)# no dot1x system-auth-control</td>
<td>Globally disables 802.1X port-based authentication.</td>
</tr>
<tr>
<td>4</td>
<td>Router(config)# aaa authorization network (\text{default} ) group radius</td>
<td>(Optional) Configures the switch to use user-RADIUS authorization for all network-related service requests such as VLAN assignment.</td>
</tr>
<tr>
<td>5</td>
<td>Router(config)# radius-server host ip-address</td>
<td>Specifies the IP address of the RADIUS server.</td>
</tr>
<tr>
<td>6</td>
<td>Router(config)# radius-server key string</td>
<td>Specifies the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
<tr>
<td>7</td>
<td>Router(config)# interface type(^1) slot/port</td>
<td>Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.</td>
</tr>
<tr>
<td>8</td>
<td>Router(config-if)# switchport mode access</td>
<td>Sets the port to access mode only if you configured the RADIUS server in previous steps.</td>
</tr>
</tbody>
</table>
Chapter 52 Configuring IEEE 802.1X Port-Based Authentication

Configuring 802.1X Port-Based Authentication

This example shows how to enable AAA and 802.1X on Fast Ethernet port 5/1:

```
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show dot1x all
```

1. type = fastethernet, gigabitethernet, or tengigabitethernet

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>Router(config-if)# dot1x port-control auto</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# no dot1x port-control auto</td>
</tr>
<tr>
<td>Step 10</td>
<td>Router(config)# end</td>
</tr>
<tr>
<td>Step 11</td>
<td>Router# show dot1x all</td>
</tr>
</tbody>
</table>

This example shows how to enable AAA and 802.1X on Gigabit Ethernet port 4/1:

```
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# dot1x system-auth-control
Router(config)# interface gigabitethernet 4/1
Router(config-if)# dot1x port-control auto
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show dot1x all
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9</td>
<td>Router(config-if)# dot1x port-control auto</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# no dot1x port-control auto</td>
</tr>
<tr>
<td>Step 10</td>
<td>Router(config)# end</td>
</tr>
<tr>
<td>Step 11</td>
<td>Router# show dot1x all</td>
</tr>
</tbody>
</table>
Configuring Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by any of the following:

- Host name
- Host IP address
- Host name and specific UDP port numbers
- 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.

To configure the RADIUS server parameters, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ip radius source-interface interface_name</code></td>
<td>Specifies that the RADIUS packets have the IP address of the indicated interface.</td>
</tr>
<tr>
<td><code>Router(config)# no ip radius source-interface</code></td>
<td>Prevents the RADIUS packets from having the IP address of the previously indicated interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>`Router(config)# radius-server host {hostname</td>
<td>ip_address}`</td>
</tr>
<tr>
<td>`Router(config)# no radius-server host {hostname</td>
<td>ip_address}`</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# radius-server key string</code></td>
<td>Configures the authorization and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.</td>
</tr>
</tbody>
</table>

When you configure the RADIUS server parameters, note the following information:

- For `hostname` or `ip_address`, specify the host name or IP address of the remote RADIUS server.
- Specify the `key string` on a separate command line.
- 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.
- When you specify the `key string`, 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 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...
Chapter 52 Configuring IEEE 802.1X Port-Based Authentication

Configuring 802.1X Port-Based Authentication

the radius-server key global configuration commands. For more information, see the Cisco IOS Security Configuration Guide, Release 12.2, publication and the Cisco IOS Security Command Reference, Release 12.2, publication at this URL:


Note

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.

This example shows how to configure the RADIUS server parameters on the switch:

Router(config)# ip radius source-interface Vlan80
Router(config)# radius-server host 172.120.39.46
Router(config)# radius-server key rad123

Enabling Multiple Hosts

You can attach multiple hosts to a single 802.1X-enabled port as shown in Figure 52-5 on page 52-8. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), all attached clients are denied access to the network.

To allow multiple hosts (clients) on an 802.1X-authorized port, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# interface type slot/port</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config-if)# dot1x port-control auto</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-if)# dot1x host-mode multi-host</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# dot1x host-mode single-host</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config-if)# end</td>
</tr>
<tr>
<td>Step 5</td>
<td>Router# show dot1x interface type slot/port</td>
</tr>
</tbody>
</table>

1. type = fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to enable 802.1X on Fast Ethernet interface 5/1 and to allow multiple hosts:

Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x host-mode multi-host

Enabling Periodic Reauthentication

With Release 12.2(33)SXH and later releases, you can enable periodic 802.1X client reauthentication and specify how often it occurs. You can specify the reauthentication period manually or you can use the session-timeout period specified by the RADIUS server. If you enable reauthentication without specifying a time period, the number of seconds between reauthentication attempts is 3600.
To enable periodic reauthentication of the client and to configure the number of seconds between reauthentication attempts, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router(config)# interface type slot/port</td>
</tr>
<tr>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config-if)# dot1x reauthentication</td>
</tr>
<tr>
<td>Enables periodic reauthentication of the client, which is disabled by default.</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# no dot1x reauthentication</td>
<td></td>
</tr>
<tr>
<td>Disables periodic reauthentication of the client.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config-if)# dot1x timeout reauth-period [seconds</td>
</tr>
<tr>
<td>Set the number of seconds between reauthentication attempts.</td>
<td></td>
</tr>
<tr>
<td>The keywords have these meanings:</td>
<td></td>
</tr>
<tr>
<td>• seconds—Sets the number of seconds from 1 to 65535; the default is 3600 seconds.</td>
<td></td>
</tr>
<tr>
<td>• server—Sets the number of seconds based on the value of the Session-Timeout RADIUS attribute (Attribute[27]) and the Termination-Action RADIUS attribute (Attribute [29]).</td>
<td></td>
</tr>
<tr>
<td>This command affects the operation of the switch only if periodic reauthentication is enabled.</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# no dot1x timeout reauth-period</td>
<td></td>
</tr>
<tr>
<td>Returns to the default reauthorization period.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config-if)# end</td>
</tr>
<tr>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Router# show dot1x interface type slot/port</td>
</tr>
<tr>
<td>Verifies your entries.</td>
<td></td>
</tr>
</tbody>
</table>

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

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 4000
```

### Manually Reauthenticating the Client Connected to a Port

**Note**

Reauthentication does not disturb the status of an already authorized port.

To manually reauthenticate the client connected to a port, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router# dot1x re-authenticate interface type slot/port</td>
</tr>
<tr>
<td>Manually reauthenticates the client connected to a port.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router# show dot1x all</td>
</tr>
<tr>
<td>Verifies your entries.</td>
<td></td>
</tr>
</tbody>
</table>

1. type = fastethernet, gigabitethernet, or tengigabitethernet
This example shows how to manually reauthenticate the client connected to Fast Ethernet port 5/1:

\[\text{Router}\# \text{dot1x re-authenticate interface fastethernet 5/1}\]

### Initializing Authentication for the Client Connected to a Port

**Note**

Initializing authentication disables any existing authentication before authenticating the client connected to the port.

To initialize the authentication for the client connected to a port, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
:\text{Router}\# \text{dot1x initialize interface type}\ slot/port | Initializes the authentication for the client connected to a port. |
| **Step 2**
:\text{Router}\# \text{show dot1x all} | Verifies your entries. |

1. type = fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to initialize the authentication for the client connected to Fast Ethernet port 5/1:

\[\text{Router}\# \text{dot1x initialize interface fastethernet 5/1}\]

### Removing 802.1X Client Information

To cause all existing supplicants to be completely deleted from an interface or from all the interfaces on the switch, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
:\text{Router}\# \text{clear dot1x interface type}\ slot/port | Removes 802.1X client information for the client connected to a port. |

:\text{Router}\# \text{clear dot1x all} | Removes 802.1X client information for all clients connected to all ports. |
| **Step 2**
:\text{Router}\# \text{show dot1x all} | Verifies your entries. |

1. type = fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to remove 802.1X client information for the client connected to Fast Ethernet port 5/1:

\[\text{Router}\# \text{clear dot1x interface fastethernet 5/1}\]
Changing 802.1X Timeouts

You can change several 802.1X timeout attributes using the `dot1x timeout {attribute} seconds` command form in the interface configuration mode. This section shows in detail how to change the quiet period timeout, followed by descriptions of how to change other 802.1X timeouts using the same command form.

Setting 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 `dot1x timeout quiet-period` interface configuration command controls the idle 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 number smaller than the default.

To change the quiet period, perform this task:

1. **Step 1**
   
   Router(config)# interface type^ slot/port
   
   Specifies the port to be configured, and enters interface configuration mode.

2. **Step 2**
   
   Router(config-if)# dot1x timeout quiet-period seconds
   
   Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client.

   Router(config-if)# no dot1x timeout quiet-period
   
   Returns to the default quiet time.

3. **Step 3**
   
   Router(config-if)# end
   
   Returns to privileged EXEC mode.

4. **Step 4**
   
   Router# show dot1x all
   
   Verifies your entries.

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

Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x timeout quiet-period 30

This example shows how to restore the default quiet period on the switch:

Router(config-if)# no dot1x timeout quiet-period

Setting the Switch-to-Client Retransmission Time

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

**Note**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific operational problems with certain clients and authentication servers.
To change the amount of time that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request, use the `dot1x timeout tx-period seconds` command in the interface configuration mode. The range is 1–65535 seconds; the default is 30. To return to the default retransmission time, use the `no dot1x timeout tx-period` command.

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

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x timeout tx-period 60
```

### Setting the Switch-to-Client Retransmission Time for EAP-Request Frames

The client notifies the switch that it received the EAP-request frame. If the switch does not receive this notification, the switch waits a set period of time and then retransmits the frame.

To set the amount of time that the switch waits for notification, use the `dot1x timeout supp-timeout seconds` command in the interface configuration mode. The range is 1–65535 seconds; the default is 30. To return to the default retransmission time, use the `no dot1x supp-timeout` command.

This example shows how to set the switch-to-client retransmission time for the EAP-request frame to 25 seconds:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x timeout supp-timeout 25
```

### Setting the Switch-to-Authentication-Server Retransmission Time for Layer 4 Packets

The authentication server notifies the switch each time it receives a Layer 4 packet. If the switch does not receive a notification after sending a packet, the switch waits a set period of time and then retransmits the packet.

To set the value for the retransmission of Layer 4 packets from the switch to the authentication server, use the `dot1x timeout server-timeout seconds` command in the interface configuration mode. The range is 1–65535 seconds; the default is 30. To return to the default retransmission time, use the `no dot1x server-timeout` command.

This example shows how to set the switch-to-authentication-server retransmission time for Layer 4 packets to 25 seconds:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x timeout server-timeout 25
```

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

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

**Note**

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific operational problems with certain clients and authentication servers.
To set the switch-to-client frame retransmission number, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>Router(config)# interface type slot/port</code></td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>Router(config-if)# dot1x max-req count</code></td>
<td>Sets the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.</td>
</tr>
<tr>
<td>Step 3: <code>Router(config-if)# no dot1x max-req</code></td>
<td>Returns to the default retransmission number.</td>
</tr>
<tr>
<td>Step 4: <code>Router(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Router# show dot1x all</code></td>
<td>Verifies your entries.</td>
</tr>
</tbody>
</table>

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

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

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x max-req 5
```

### Setting the Reauthentication Number

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>Router(config)# interface type slot/port</code></td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 2: <code>Router(config-if)# dot1x max-reauth-req count</code></td>
<td>Sets the number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 0 to 10; the default is 2.</td>
</tr>
<tr>
<td>Step 3: <code>Router(config-if)# no dot1x max-reauth-req</code></td>
<td>Returns to the default reauthentication number.</td>
</tr>
<tr>
<td>Step 4: <code>Router(config-if)# end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Router# show dot1x all</code></td>
<td>Verifies your entries.</td>
</tr>
</tbody>
</table>

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

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:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x max-reauth-req 4
```
Configuring IEEE 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 then can determine that all active 802.1X sessions are closed.

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

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

When the stop message is not sent successfully, this message appears:

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

**Note**

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

To configure 802.1X accounting after AAA is enabled on your switch, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router(config)# aaa accounting dot1x default start-stop group radius</td>
</tr>
<tr>
<td>Enables 802.1X accounting using the list of all RADIUS servers.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config)# aaa accounting system default start-stop group radius</td>
</tr>
<tr>
<td>(Optional) Enables system accounting (using the list of all RADIUS servers) and generates system accounting reload event messages when the switch reloads.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config)# end</td>
</tr>
<tr>
<td>Returns to privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router# show running-config</td>
</tr>
<tr>
<td>Verifies your entries.</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

Configuring a Guest VLAN

With Release 12.2(33)SXH and later releases, 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. When operating as a guest VLAN, a port functions in multiple-hosts mode regardless of the configured host mode of the port.
To configure a guest VLAN, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# interface type slot/port</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config-if)# switchport mode access</td>
</tr>
<tr>
<td></td>
<td>or Router(config-if)# switchport mode private-vlan</td>
</tr>
<tr>
<td></td>
<td>host</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-if)# dot1x port-control auto</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config-if)# dot1x guest-vlan vlan-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>Router(config-if)# end</td>
</tr>
<tr>
<td>Step 6</td>
<td>Router# show dot1x interface type slot/port</td>
</tr>
</tbody>
</table>

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

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

Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x guest-vlan 2

This example shows how to set 3 seconds as the client notification timeout 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 re-sending the request, and to enable VLAN 2 as an 802.1X guest VLAN when an 802.1X port is connected to a DHCP client:

Router(config-if)# dot1x timeout supp-timeout 3
Router(config-if)# dot1x timeout tx-period 15
Router(config-if)# dot1x guest-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. When operating as a restricted VLAN, a port functions in single-host mode regardless of the configured host mode of the port.
To configure a restricted VLAN, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;Router(config)# interface type slot/port</td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;Router(config-if)# switchport mode access or&lt;br&gt;Router(config-if)# switchport mode private-vlan host</td>
<td>Sets the port to access mode, or Configures the port as a private-VLAN host port.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;Router(config-if)# dot1x port-control auto</td>
<td>Enables 802.1X authentication on the port.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;Router(config-if)# dot1x auth-fail vlan vlan-id</td>
<td>Specifies an active VLAN as an 802.1X restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, a private primary PVLAN, or a voice VLAN as an 802.1X restricted VLAN.</td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;Router(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong>&lt;br&gt;Router# show dot1x interface type slot/port</td>
<td>Verifies your entries.</td>
</tr>
</tbody>
</table>

1. type = fastethernet, gigabitethernet, or tengigabitethernet

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

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

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x auth-fail vlan 2
```

You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the **dot1x auth-fail max-attempts** interface configuration command. The range of allowable authentication attempts is 1 to 3. The default is 3 attempts.

To configure the maximum number of allowed authentication attempts, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;Router(config)# interface type slot/port</td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;Router(config-if)# switchport mode access or&lt;br&gt;Router(config-if)# switchport mode private-vlan host</td>
<td>Sets the port to access mode, or Configures the port as a private-VLAN host port.</td>
</tr>
<tr>
<td><strong>Step 3</strong>&lt;br&gt;Router(config-if)# dot1x port-control auto</td>
<td>Enables 802.1X authentication on the port.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;Router(config-if)# dot1x auth-fail vlan vlan-id</td>
<td>Specifies an active VLAN as an 802.1X restricted VLAN. The range is 1 to 4094. You can configure any active VLAN except an internal VLAN (routed port), an RSPAN VLAN, a private primary PVLAN, or a voice VLAN as an 802.1X restricted VLAN.</td>
</tr>
</tbody>
</table>
To return to the default value, use the `no dot1x auth-fail max-attempts` interface configuration command.

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

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x auth-fail max-attempts 2
```

### Configuring the Inaccessible Authentication Bypass Feature

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

To configure the port as a critical port and enable the inaccessible authentication bypass feature, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# <code>radius-server dead-criteria time time tries tries</code> (Optional) Sets the conditions that are used to decide when a RADIUS server is considered unavailable or dead. The range for <code>time</code> is from 1 to 120 seconds. The switch dynamically determines the default <code>seconds</code> value that is 10 to 60 seconds. The range for <code>tries</code> is from 1 to 100. The switch dynamically determines the default <code>tries</code> parameter that is 10 to 100.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# <code>radius-server deadtime minutes</code> (Optional) Sets 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.</td>
</tr>
</tbody>
</table>
Step 3

```
Router(config)# radius-server host ip-address [acct-port udp-port] [auth-port udp-port] [key string] [test username name] [idle-time time] [ignore-acct-port] [ignore-auth-port]
```

(Optional) Configures 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.

- **key string**—Specify the authentication and encryption key for all RADIUS communication between the switch and the RADIUS daemon.

**Note**

You can also configure the authentication and encryption key by using the `radius-server key {0 string | 7 string | string} global configuration command`.

- **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.

Step 4

```
Router(config)# dot1x critical [eapol | recovery delay milliseconds]
```

(Optional) Configures the parameters for inaccessible authentication bypass:

- **eapol**—Specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.
- **recovery delay milliseconds**—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 5

```
Router(config)# interface type slot/port
```

Specifies the port to be configured, and enters interface configuration mode.
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** global configuration command. To disable inaccessible authentication bypass, use the **no dot1x critical** interface configuration command.

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

```plaintext
Router(config)# radius-server dead-criteria time 30 tries 20
Router(config)# radius-server deadtime 60
Router(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 key abc1234 test
username user1 idle-time 30
Router(config)# dot1x critical eapol
Router(config)# dot1x critical recovery delay 2000
Router(config)# interface gigabitethernet 0/1
Router(config-if)# dot1x critical
Router(config-if)# dot1x critical recovery action reinitialize
```

### Configuring 802.1X Authentication with WoL

To enable 802.1X authentication with wake-on-LAN (WoL), perform this task:

```plaintext
Step 1
Router(config)# interface type1 slot/port

Step 2
Router(config-if)# dot1x control-direction {both | in}

Enables 802.1X authentication with 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 3
Router(config-if)# end

Step 4
Router# show dot1x interface type slot/port

Verifies your entries.
```

1. **type** = fastethernet, gigabitethernet, or tengigabitethernet
To disable 802.1X authentication with WoL, use the `no dot1x control-direction` interface configuration command.

This example shows how to enable 802.1X authentication with WoL and set the port as bidirectional:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x control-direction both
```

### Configuring MAC Authentication Bypass

To enable MAC authentication bypass, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>Router(config)# interface type slot/port</code>&lt;br&gt;Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`Router(config-if)# dot1x port-control {auto</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>Router(config-if)# dot1x mac-auth-bypass [eap]</code>&lt;br&gt;Enables MAC authentication bypass.&lt;br&gt;(Optional) Use the <code>eap</code> keyword to configure the switch to use EAP for authorization.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>Router(config-if)# end</code>&lt;br&gt;Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>Router# show dot1x interface type slot/port</code>&lt;br&gt;Verifies your entries.</td>
</tr>
</tbody>
</table>

1. `type = fastethernet, gigabitethernet, or tengigabitethernet`

**Note**

To use MAC authentication bypass on a routed port, make sure that MAC address learning is enabled on the port.

This example shows how to enable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x mac-auth-bypass
```
## Configuring NAC Layer 2 IEEE 802.1X Validation

With Cisco IOS Release 12.2(33)SXH or later, you can configure NAC Layer 2 IEEE 802.1X validation, which is also referred to as 802.1X authentication with a RADIUS server. NAC Layer 2 IEEE 802.1X configuration is the same as 802.1X configuration with the additional step of configuring the RADIUS server with a posture token and VLAN assignment.

To configure NAC Layer 2 IEEE 802.1X validation, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# interface type $ slot/port</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config-if)# dot1x port-control auto</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-if)# dot1x reauthentication</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config-if)# dot1x timeout reauth-period {seconds</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Router(config-if)# end</td>
</tr>
<tr>
<td>Step 6</td>
<td>Router# show dot1x interface type slot/port</td>
</tr>
</tbody>
</table>

1. type = fastethernet, gigabitethernet, or tengigabitethernet

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

```
Router(config)# interface fastethernet 5/1
Router(config)# dot1x port-control auto
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period server
```
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.

To disable 802.1X authentication on the port, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Router(config)# interface type\ slot/port</td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 2: Router(config-if)# no dot1x pae</td>
<td>Disables 802.1X authentication on the port.</td>
</tr>
<tr>
<td>Step 3: Router(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4: Router# show dot1x interface type slot/port</td>
<td>Verifies your entries.</td>
</tr>
</tbody>
</table>

1. `type` = fastethernet, gigabitethernet, or tengigabitethernet

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

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

```
Router(config)# interface fastethernet 5/1
Router(config-if)# no dot1x pae authenticator
```

Resetting the 802.1X Configuration to the Default Values

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Router(config)# interface type\ slot/port</td>
<td>Specifies the port to be configured, and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 2: Router(config-if)# dot1x default</td>
<td>Resets the configurable 802.1X parameters to the default values.</td>
</tr>
<tr>
<td>Step 3: Router(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4: Router# show dot1x all</td>
<td>Verifies your entries.</td>
</tr>
</tbody>
</table>

1. `type` = fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to reset a port’s 802.1X authentication settings to the default values:

```
Router(config)# interface gigabitethernet 3/27
Router(config-if)# dot1x default
```
Displaying 802.1X Status

To display the global 802.1X administrative and operational status for the switch or the 802.1X settings for individual ports, perform this task:

### Command

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
|        | `Router# show dot1x [all | Displays the global 802.1X administrative and operational status for |[
|        |   interface                 | the switch. (Optional) Use the `all` keyword to display the global   |[
|        | type slot/port]             | 802.1X status and the 802.1X settings for all interfaces using         |[
|        |                             | 802.1X authentication. (Optional) Use the `interface` keyword to display |[
|        |                             | the 802.1X settings for a specific interface.                          |[
|        |                             |                                                                         |
|        |                             |                                                                         |
| 1.     | `type` = `fastethernet`,   |                                                                         |
|        | `gigabitethernet`, or `tengigabitethernet` |                                                                         |

This example shows how to view only the global 802.1X status:

```
Router# show dot1x
Sysauthcontrol       Disabled
Dot1x Protocol Version 2
Critical Recovery Delay 100
Critical EAPOL       Disabled

Router#
```

This example shows how to view the global 802.1X status and the 802.1X settings for all interfaces using 802.1X authentication:

```
Router# show dot1x all
Sysauthcontrol       Disabled
Dot1x Protocol Version 2
Critical Recovery Delay 100
Critical EAPOL       Disabled

Dot1x Info for GigabitEthernet3/27
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0

Router#
```

For detailed information about the fields in these displays, see the Cisco IOS Software Releases 12.2SX Command References.