# Configuring IEEE 802.1x Port-Based Authentication

**Last Updated: July 20, 2011**

This document describes how to configure IEEE 802.1x port-based authentication on Cisco integrated services routers (ISRs). IEEE 802.1x authentication prevents unauthorized devices (supplicants) from gaining access to the network.

Cisco ISRs can combine the functions of a router, a switch, and an access point, depending on the fixed configuration or installed modules. The switch functions are provided by either built in switch ports or a plug-in module with switch ports.

**Note** This document describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.



# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Prerequisites for Configuring IEEE 802.1x Port-Based Authentication

The features described in this document are available only on switch ports installed in Cisco ISR routers. The IEEE 802.1x port-based authentication features are available in Cisco IOS Release 12.4(11)T on Cisco 800, 870, 1800, 2800, and 3800 series ISRs that support switch ports.

The fixed configuration Cisco 1800 series router platforms and the Cisco 870 series routers have integrated 4-port and 8-port switches.

The following cards or modules support switch ports:

- High-speed WAN interface cards (HWIC)
  - HWIC-4ESW
  - HWICD-9ESW
- EtherSwitch Network Modules
  - NM-16ESW
  - NMD-36ESW

**Note** Not all Cisco ISR routers support all the components listed. For information about module compatibility with a specific router platform, see Cisco EtherSwitch Modules Comparison .

To determine whether your router has switch ports that can be configured with the IEEE 802.1x port-based authentication feature, use the **show interfaces switchport**command.

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

# Restrictions for Configuring IEEE 802.1x Port-Based Authentication



## IEEE 802.1x Authentication Configuration Restrictions

- When IEEE 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 (for example, from access to trunk) of an IEEE 802.1x-enabled port, an error message appears, and the port mode is not changed.
- If the VLAN to which an IEEE 802.1x-enabled port is assigned changes, this change is transparent and does not affect the switch port. 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 IEEE 802.1x port is assigned is 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 IEEE 802.1x protocol is supported on Layer 2 static-access ports, voice VLAN enabled ports, and Layer 3 routed ports, but it is not supported on these port types:
  - Dynamic-access ports--If you try to enable IEEE 802.1x authentication on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
  - Dynamic ports--If you try to enable IEEE 802.1x authentication on a dynamic port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to dynamic, an error message appears, and the port mode is not changed.
  - Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports--You can enable IEEE 802.1x authentication on a port that is a SPAN or RSPAN destination port. However, IEEE 802.1x authentication is disabled until the port is removed as a SPAN or RSPAN destination port. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.
  - Trunk port--If you try to enable IEEE 802.1x authentication on a trunk port, an error message appears, and IEEE 802.1x authentication is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, an error message appears, and the port mode is not changed.

**Note** A port in dynamic mode can negotiate with its neighbor to become a trunk port.

# VLAN Assignment Configuration Restrictions

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

# Guest VLAN Configuration Restrictions

- You can configure any VLAN except an RSPAN VLAN or a voice VLAN as an IEEE 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 IEEE 802.1x port to which a DHCP client is connected, you might have to get a host IP address from a DHCP server. You can change the settings for restarting the IEEE 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 IEEE 802.1x authentication process (using the **dot1x max-reauth-req** and **dot1x timeout tx-period** interface configuration commands). The amount of decrease depends on the connected IEEE 802.1x client type.

# Upgrading from a Previous Software Release

In Cisco IOS Release 12.4(11)T, the implementation for IEEE 802.1x authentication changed from the previous releases. When IEEE 802.1x authentication is enabled, information about Port Fast is no longer added to the configuration.

**Note** When you enter any IEEE 802.1x-related commands on a port, this information is automatically added to the running configuration to address any backward compatibility issues: dot1xpae authenticator

# Information About IEEE 802.1x Port-Based Authentication

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

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

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


- IEEE 802.1x Authenticator, page 4
- IEEE 802.1x with RADIUS Accounting, page 8

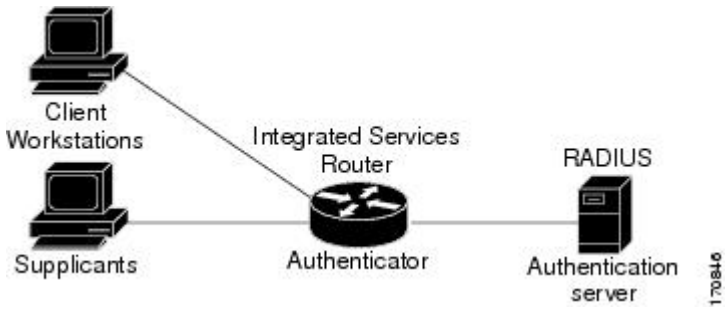

# IEEE 802.1x Authenticator


- Device Roles, page 4
- Authentication Initiation and Message Exchange, page 5
- Authentication Process, page 6
- Ports in Authorized and Unauthorized States, page 7
- IEEE 802.1x Host Mode, page 8


## Device Roles

With IEEE 802.1x port-based authentication, the devices in the network have specific roles as shown in the figure below.

***Figure 1***



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

**Note** To resolve Windows XP network connectivity and IEEE 802.1x authentication issues, read the Microsoft Knowledge Base article at this URL: http://support.microsoft.com/kb/q303597/

- *Authentication server* --Device that performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services. The Network Access Device (or ISR router in this instance) transparently passes the authentication messages between the supplicant and the authentication server, and the authentication process is carried out between the supplicant and the authentication server. The particular EAP method used will be decided between the supplicant and the authentication server (RADIUS server). The RADIUS security system with EAP extensions is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client and server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- *Authenticator (integrated services router (* ISR) or wireless access point)--Router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

When the authenticator receives EAPOL frames and relays them to the authentication server, the EAPOL is stripped and the remaining EAP frame is reencapsulated in the RADIUS format. The EAP frames are not modified during encapsulation, and the authentication server must support EAP within the native frame format. When the authenticator 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 Initiation and Message Exchange

During IEEE 802.1x authentication, the router or the supplicant can initiate authentication. If you enable authentication on a port by using the **dot1x port-control auto** interface configuration command, the router initiates authentication when the link state changes from down to up or periodically if the port remains up and unauthenticated. The router sends an EAP-request/identity frame to the supplicant to request its identity. Upon receipt of the frame, the supplicant responds with an EAP-response/identity frame.

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

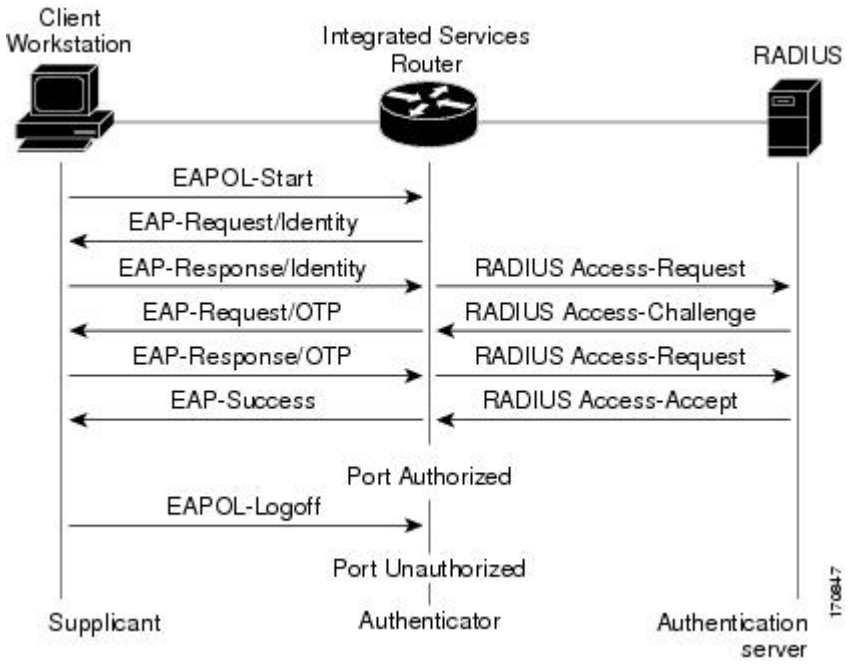
**Note** If IEEE 802.1x authentication is not enabled or supported on the network access device, any EAPOL frames from the supplicant are dropped. If the supplicant does not receive an EAP-request/identity frame after three attempts to start authentication, the supplicant sends frames as if the port is in the authorized state. A port in the authorized state effectively means that the supplicant has been successfully authenticated. For more information, see the Ports in Authorized and Unauthorized States module.

When the supplicant supplies its identity, the router begins its role as the intermediary, passing EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the

authentication succeeds, the router 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 module.

The specific exchange of EAP frames depends on the authentication method being used. The figure below shows a message exchange initiated by the supplicant using the One-Time-Password (OTP) authentication method with a RADIUS server.

***Figure 2***




## Authentication Process

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

The AAA process begins with authentication. When IEEE 802.1x port-based authentication is enabled and the device attempting to authenticate is IEEE 802.1x-capable (meaning it supports the supplicant functionality) these events occur:

- If the supplicant identity is valid and the IEEE 802.1x authentication succeeds, the router grants the supplicant access to the network.

The router reauthenticates a supplicant when one of these situations occurs:

- Periodic reauthentication is enabled, and the reauthentication timer expires.

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

After IEEE 802.1x authentication using a RADIUS server is configured, the router 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.

The Termination-Action RADIUS attribute (Attribute [29]) specifies the action to take during reauthentication. The actions can be *Initialize* or *ReAuthenticate* . When the *Initialize* action is set (the attribute value is *DEFAULT* ), the IEEE 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 supplicant by entering the **dot1x re-authenticate interface***interface-id* privileged EXEC command.

## Ports in Authorized and Unauthorized States

During IEEE 802.1x authentication, depending on the port state, the router can grant a supplicant access to the network. The port starts in the *unauthorized* state. While in this state, the port that is not configured as a voice VLAN port disallows all ingress traffic except for IEEE 802.1x authentication, CDP, and STP packets. When a supplicant is successfully authenticated, the port changes to the *authorized* state, allowing all traffic for the supplicant to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and IEEE 802.1x protocol packets before the supplicant is successfully authenticated.

If a client that does not support IEEE 802.1x authentication connects to an unauthorized IEEE 802.1x port, the router requests the client's identity. In this situation, if 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 IEEE 802.1x-enabled supplicant connects to a port that is not running the IEEE 802.1x standard, the supplicant initiates the authentication process by sending the EAPOL-start frame. When no response is received, the supplicant sends the request for a fixed number of times. Because no response is received, the supplicant 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 IEEE 802.1x authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 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 supplicant to authenticate. The router cannot provide authentication services to the supplicant through the port.
- **auto** --Enables IEEE 802.1x authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The router requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the router by using the supplicant MAC address.

If the supplicant is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated supplicant 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 router can resend the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

When a supplicant logs off, it sends an EAPOL-logoff message, causing the router port to change to the unauthorized state.

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

For information about configuring IEEE 802.1x port-based authentication, see the “Configuring IEEE 802.1x Authentication” section of the “Configuring IEEE 802.1x Port-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE* .

## IEEE 802.1x Host Mode

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

You can configure an IEEE 802.1x port for single-host or for multi-host mode. In single-host mode (see the figure IEEE 802.1x Device Roles in the Device Roles section of this module), only one supplicant can be authenticated by the IEEE 802.1x-enabled switch port. The router detects the supplicant by sending an EAPOL frame when the port link state changes to the up state. If a supplicant leaves or is replaced with another supplicant, the router changes the port link state to down, and the port returns to the unauthorized state.

In multi-host mode, you can attach multiple hosts to a single IEEE 802.1x-enabled port. In this mode, only one of the attached supplicants must be authorized for all supplicants to be granted network access. If the port becomes unauthorized (reauthentication fails or an EAPOL-logoff message is received), the router denies network access to all of the attached supplicants.

**Note** Cisco 870 series platforms do not support single-host mode.

For information about configuring IEEE 802.1x host mode, see the “Configuring the Host Mode” section of the “Configuring IEEE 802.1x Port-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE* .

# IEEE 802.1x with RADIUS Accounting

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.



## IEEE 802.1x RADIUS Accounting

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

**Note** To enable IEEE 802.1x accounting, you must first configure IEEE 802.1x authentication and switch-to-RADIUS server communication.

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

**Note** You must configure the IEEE 802.1x supplicant to send an EAP-logoff (Stop) message to the switch when the user logs off. If you do not configure the IEEE 802.1x supplicant, an EAP-logoff message is not sent to the switch and the accompanying accounting Stop message is not sent to the authentication server. See the Microsoft Knowledge Base article at the location: http://support.microsoft.com and set the SupplicantMode registry to 3 and the AuthMode registry to 1.

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

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

- User successfully authenticates.
- User logs off.
- Link-down occurs on an IEEE 802.1x port.
- Reauthentication succeeds.
- Reauthentication fails.

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

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

This is the IEEE 802.1x RADIUS accounting process

1. A user connects to a port on the router.
2. Authentication is performed.
3. VLAN assignment is enabled, as appropriate, based on the RADIUS server configuration.
4. The router sends a start message to an accounting server.
5. Reauthentication is performed, as necessary.
6. The port 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 router sends a stop message to the accounting server.

The switch port 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.

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

- Enable accounting in your RADIUS server.
- Enable IEEE 802.1x accounting on your switch.
- Enable AAA accounting by using the **aaa system accounting** command.

Enabling AAA system accounting along with IEEE 802.1x accounting allows system reload events to be sent to the accounting RADIUS server for logging. When the accounting RADIUS server receives notice of a system reload event, the server can infer that all active IEEE 802.1x sessions are appropriately closed.

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

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

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

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

**Note** Use the **debug radius** command or **debug radius accounting** command to enable the %RADIUS-3-NO ACCOUNTING RESPONSE message.

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

For information about configuring IEEE 802.1x RADIUS accounting, see the “Enabling 802.1X Accounting” section of the “Configuring 802.1X Port-Based Authentication” chapter in the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*, 12.2(31)SGA.

## IEEE 802.1x Accounting Attribute-Value Pairs

The information sent to the RADIUS server is represented in the form of 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 router that is configured for IEEE 802.1x accounting. Three types of RADIUS accounting packets are sent by a router:

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

The following table lists the AV pairs and when they are sent by the router:

***Table 1 Accounting AV Pairs***

| Attribute Number | AV Pair Name | START | INTERIM | STOP |
|---|---|---|---|---|
| Attribute[1] | User-Name | Always | Always | Always |
| Attribute[4] | NAS-IP-Address | Always | Always | Always |
| Attribute[5] | NAS-Port | Always | Always | Always |
| Attribute[6] | Service-Type | Always | Always | Always |
| Attribute[8] | Framed-IP-Address | Never | Sometimes[1] | Sometimes 1 |

| Attribute Number | AV Pair Name | START | INTERIM | STOP |
|---|---|---|---|---|
| Attribute[25] | Class | Always | Always | Always |
| Attribute[30] | Called-Station-ID | Always | Always | Always |
| Attribute[31] | Calling-Station-ID | Always | Always | Always |
| Attribute[40] | Acct-Status-Type | Always | Always | Always |
| Attribute[41] | Acct-Delay-Time | Always | Always | Always |
| Attribute[42] | Acct-Input-Octets | Never | Always | Always |
| Attribute[43] | Acct-Output-Octets | Never | Always | Always |
| Attribute[44] | Acct-Session-ID | Always | Always | Always |
| Attribute[45] | Acct-Authentic | Always | Always | Always |
| Attribute[46] | Acct-Session-Time | Never | Never | Always |
| Attribute[47] | Acct-Input-Packets | Never | Always | Always |
| Attribute[48] | Acct-Output-Packets | Never | Always | Always |
| Attribute[49] | Acct-Terminate-Cause | Never | Never | Always |
| Attribute[61] | NAS-Port-Type | Always | Always | Always |

You can configure the ISR to send Cisco vendor-specific attributes (VSAs) to the RADIUS server. The following table lists the available Cisco AV pairs.

**Note** To enable VSAs to be sent in the accounting records you must configure the **radius-server vsa send accounting** command.

***Table 2 Cisco Vendor-Specific Attributes***

| Attribute Number | AV Pair Name | START | INTERIM | STOP |
|---|---|---|---|---|
| Attribute[26,9,1] | Cisco-Avpair: connect-progress | Always | Always | Always |
| Attribute[26,9,2] | cisco-nas-port | Always | Always | Always |
| Attribute[26,9,1] | Cisco-Avpair: disc-cause | Never | Never | Always |

You can view the AV pairs that are being sent by the router by entering the **debug radius accounting** privileged EXEC command. For more information about this command, see the *Cisco IOS Debug*

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

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

# How to Use IEEE 802.1x Authentication with Other Features



## IEEE 802.1x Authentication with VLAN Assignment

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

In Cisco IOS Release 12.4(11)T and later releases, the switch ports support IEEE 802.1x authentication with VLAN assignment. After successful IEEE 802.1x authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. You can use the VLAN Assignment feature to limit network access for certain users.

The RADIUS server database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the supplicant connected to the switch port.

This section contains the following information about IEEE 802.1x VLAN assignment:



### Prerequisites for IEEE 802.1x VLAN Assignment

- IEEE 802.1x must be enabled on the switch port.
- EAP support must be enabled on the RADIUS server.
- AAA authorization must be configured on the port for all network-related service requests.
- The port must be successfully authenticated.

### Restrictions for IEEE 802.1x VLAN Assignment

- The switch port is always assigned to the configured access VLAN when any of the following conditions occurs:
  - No VLAN is supplied by the RADIUS server.
  - The VLAN information from the RADIUS server is not valid.
  - IEEE 802.1x authentication is disabled on the port.
  - The port is in the force authorized, force unauthorized, unauthorized, or shutdown state.

**Note** An access VLAN is a VLAN assigned to an access port. All packets sent from or received on this port belong to this VLAN.

- Assignment to the configured access VLAN prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error. Examples of configuration errors include the following:
  - A nonexistent or malformed VLAN ID
  - Attempted assignment to a voice VLAN ID
- The IEEE 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).
- If the multi-host mode is enabled on an IEEE 802.1x port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- If an IEEE 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.

## Configuring VLAN Assignment

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

- Enable AAA authorization by using the **network** keyword to allow interface configuration from the RADIUS server. For detailed instructions, see the Configuring RADIUS Authorization for User Privileged Access and Network Services section of the Configuring Switch-Based Authentication chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE* .
- Enable IEEE 802.1x authentication. For detailed instructions, see the Configuring RADIUS Login Authentication section of the Configuring Switch-Based Authentication chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE* .

**Note** The VLAN assignment feature is automatically enabled when you configure IEEE 802.1x authentication on an access port.

- Assign vendor-specific tunnel attributes in the RADIUS server. The RADIUS server must return these attributes to the router:
  - [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 IEEE 802.1x-authenticated user.

For examples of tunnel attributes, see the Configuring the Switch to Use Vendor-Specific RADIUS Attributes section of the Configuring Switch-Based Authentication chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE* .

# IEEE 802.1x Authentication with Guest VLAN

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

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

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

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

In Cisco IOS Release 12.4(11)T and later releases, if devices send EAPOL packets to the router during the lifetime of the link, the router does not allow clients that fail authentication access to the guest VLAN.

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

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

Guest VLANs are supported on IEEE 802.1x ports in single-host or multi-host mode.

You can configure any active VLAN except a remote switch port analyzer (RSPAN) VLAN or a voice VLAN as an IEEE 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.

For information about configuring a guest VLAN, see the “Configuring a Guest VLAN”section of the “Configuring IEEE 802.1x Port-Based Authentication” chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE* .

# IEEE 802.1x with RADIUS-Supplied Session Timeout

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

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

If the switch port is configured to use the RADIUS-provided timeout, it looks in the RADIUS Access-Accept message for the Session-Timeout and optional Termination-Action attributes. The switch port uses

the value of the Session-Timeout attribute to determine the duration of the session, and it uses the value of the Termination-Action attribute to determine the switch action when the session's timer expires.

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

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

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

# IEEE 802.1x Authentication with Voice VLAN Ports

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

A voice VLAN port is a special access port 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 router through the IP phone. The PVID is the native VLAN of the port.

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 IEEE 802.1x authentication.

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

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 router recognizes only the one directly connected to it. When IEEE 802.1x authentication is enabled on a voice VLAN port, the router drops packets from unrecognized IP phones more than one hop away.

When IEEE 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 IEEE 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 router for up to 30 seconds.

For information about configuring IEEE 802.1x with voice VLANs, see " Configuring Voice VLAN" in the Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE.

# Enabling IEEE 802.1x SNMP Notifications on Switch Ports

**Note** This section describes IEEE 802.1x security features available only on the switch ports in a Cisco ISR.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps dot1x** *notification-type*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables higher privilege levels, such as privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server enable traps dot1x** *notification-type*<br><br>**Example:**<br>`Router (config)# snmp-server enable traps dot1x no-guest-vlan` | Enables SNMP logging and reporting when no Guest VLAN is configured or available. |

# IEEE 802.1x MIB Support

Cisco IOS Release 12.4(11)T provides support for the following MIBs that provide SNMP access to IEEE 802.1x feature components:

- IEEE8021-PAE-MIB
- Cisco-PAE-MIB

The IEEE8021-PAE-MIB supports reporting of the following information:

- The state of the IEEE 802.1x state machine on a particular port
- Statistics associated with the state of the IEEE 802.1x state machine

The Cisco-PAE-MIB provides SNMP support for the logging and reporting of events, including:

- Port mode

- Guest VLAN number (Details the Guest VLAN number configured on a port.)
- InGuestVLAN (Indicates whether a port is in the Guest VLAN.)

# Configuration Examples for IEEE 802.1x Features



## Enabling IEEE 802.1x and AAA on a Port Example

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

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

```
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface fastethernet2/1
Router(config-if)# switchport mode access
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x port-control auto
Router(config-if)# end
Router# show dot1x interface fastethernet7/1 details
Dot1x Info for FastEthernet7/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Dot1x Authenticator Client List
-------------------------------
Supplicant                = 1000.0000.2e00
        Auth SM State     = AUTHENTICATED
        Auth BEND SM Stat = IDLE
Port Status               = AUTHORIZED

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

# Enabling IEEE 802.1x RADIUS Accounting Example

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server. The first command configures the RADIUS server, specifying port 1612 as the authorization port, 1813 as the UDP port for accounting, and rad123 as the encryption key:

```
Router# configure terminal
Router(config)# radius-server host 172.20.39.46 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
Router(config)# end
Router#
```

**Note** You must configure the RADIUS server to perform accounting tasks.

# Configuring IEEE 802.1x with Guest VLAN Example

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

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

# Configuring RADIUS-Provided Session Timeout Example

This example assumes you have enabled IEEE 802.1x reauthentication and shows how to configure the switch port to derive the reauthentication period from the server and to verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet7/1
Router(config-if)# switchport mode access
Router(config-if)# dot1x pae authenticator
Router(config-if)# dot1x timeout reauth-period server
Router(config-if)# end
Router#
```

# Configuring IEEE 802.1x with Voice VLAN Example

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

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

# Displaying IEEE 802.1x Statistics and Status Example

To display IEEE 802.1x statistics for all ports, use the **show dot1x all statistics** privileged EXEC command. To display IEEE 802.1x statistics for a specific port, use the **show dot1x statistics interface***interface-id* privileged EXEC command.

To display the IEEE 802.1x administrative and operational status for the switch, use the **show dot1x all**[**details** | **statistics**| **summary**] privileged EXEC command. To display the IEEE 802.1x administrative and operational status for a specific port, use the **show dot1x interface***interface-id* privileged EXEC command. For detailed information about the fields in these displays, see the command reference for this release.

This example shows the output of the **show dot1x all**command:

```
Router-871# show dot1x all
Sysauthcontrol                  Enabled
Dot1x Protocol Version     2
Dot1x Info for FastEthernet1
---------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Disabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3600 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
RateLimitPeriod           = 0
Router-871#
```

This example shows the output of the **show dot1x summary**command:

```
Router-871# show dot1x all summary

Interface             PAE             Client                          Status
-----------------------------------------------------------------------------------------
Fa1                   AUTH             000d.bcef.bfdc           AUTHORIZED
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Configuring IEEE 802.1x Port-Based Authentication | The chapter Configuring 802.1X Port-Based Authentication in the *Catalyst 3750 Series Switch Cisco IOS Software Configuration Guide* , 12.2(31)SEE |

| Related Topic | Document Title |
|---|---|
| IEEE 802.1x commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | • *Catalyst 4500 Series Switch Cisco IOS Command Reference, Release 12.2(25)SGA*<br>• *Catalyst 3750 Switch Command Reference , Cisco IOS Release 12.2(25)SEE* |
| VPN Access Control Using IEEE 802.1x Authentication | The VPN Access Control Using 802.1X Authentication feature module. |

### Standards

| Standard | Title |
|---|---|
| IEEE 802.1x | *Port Based Network Access Control* |

### MIBs

| MIB | MIBs Link |
|---|---|
| • IEEE8021-PAE-MIB<br>• Cisco-PAE-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| RFC 3580 | *IEEE 802.1x Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Configuring IEEE 802.1x Port-Based Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 3 Feature Information for Configuring IEEE 802.1x Port-Based Authentication***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE 802.1x Authenticator | 12.3(4)T | This feature was introduced to prevent unauthorized devices (supplicants) from gaining access to the network.<br><br>This feature is available on the following Cisco ISRs equipped with cards or modules that include switch ports:<br><br>• Cisco 800 Series ISR<br>• Cisco 870 Series ISR<br>• Cisco 1800 Series ISR<br>• Cisco 2800 Series ISR<br>• Cisco 3800 Series ISR<br><br>In Cisco IOS Release 12.4(11)T, this feature was modified to include the other features listed in this table.<br><br>The following commands were introduced or modified: **aaa accounting , dot1x guest-vlan , snmp-server enable traps**. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE 802.1x RADIUS Accounting | 12.4(11)T | This feature relays important events to the RADIUS server (such as the supplicant's connection session). This information is used for security and billing purposes.<br>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:<br>• Cisco 800 Series ISR<br>• Cisco 870 Series ISR<br>• Cisco 1800 Series ISR<br>• Cisco 2800 Series ISR<br>• Cisco 3800 Series ISR |
| IEEE 802.1x--VLAN Assignment | 12.4(11)T | This feature allows the RADIUS server to send the VLAN assignment to configure the switch port.<br>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:<br>• Cisco 800 Series ISR<br>• Cisco 870 Series ISR<br>• Cisco 1800 Series ISR<br>• Cisco 2800 Series ISR<br>• Cisco 3800 Series ISR |

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE 802.1x Guest VLAN | 12.4(11)T | This feature allows you to configure a guest VLAN for each IEEE 802.1x-capable switch port on the router to provide limited services to clients, such as downloading the IEEE 802.1x client.<br><br>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:<br><br>• Cisco 800 Series ISR<br>• Cisco 870 Series ISR<br>• Cisco 1800 Series ISR<br>• Cisco 2800 Series ISR<br>• Cisco 3800 Series ISR |
| IEEE 802.1x RADIUS-Supplied Session Timeout | 12.4(11)T | This feature allows you to specify whether a switch port uses a locally configured or a RADIUS-provided reauthentication timeout.<br><br>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:<br><br>• Cisco 800 Series ISR<br>• Cisco 870 Series ISR<br>• Cisco 1800 Series ISR<br>• Cisco 2800 Series ISR<br>• Cisco 3800 Series ISR |

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE 802.1x--Voice VLAN | 12.4(11)T | This feature allows you to configure a special access port associated with two VLAN identifiers:<br>• 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.<br>• Port VLAN identifier (PVID) to carry the data traffic to and from the workstation connected to the router through the IP phone. The PVID is the native VLAN of the port.<br>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:<br>• Cisco 800 Series ISR<br>• Cisco 870 Series ISR<br>• Cisco 1800 Series ISR<br>• Cisco 2800 Series ISR<br>• Cisco 3800 Series ISR |
| IEEE 802.1x MIB Support | 12.4(11)T | This feature provides support for the following MIBs:<br>• IEEE8021-PAE-MIB<br>• Cisco-PAE-MIB<br>In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports:<br>• Cisco 800 Series ISR<br>• Cisco 870 Series ISR<br>• Cisco 1800 Series ISR<br>• Cisco 2800 Series ISR<br>• Cisco 3800 Series ISR |