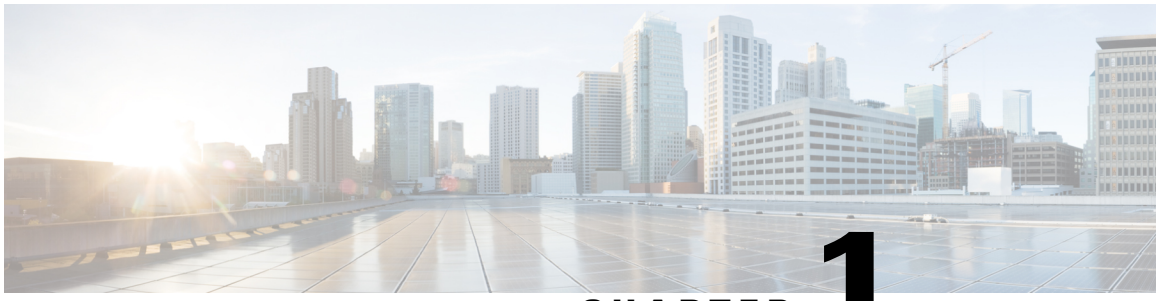
# 802.1X Authentication Services Configuration Guide, Cisco IOS Release 15SY

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS



CHAPTER 1

# Configuring IEEE 802.1X Port-Based Authentication

IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network. The device can combine the function of a router, switch, and 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. This feature supports both access ports and trunk ports.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 following tasks must be completed before implementing the IEEE 802.1X Port-Based Authentication feature:

- IEEE 802.1X must be enabled on the device port.
- The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs).
- EAP support must be enabled on the RADIUS server.
- 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.
- Authentication, authorization, and accounting (AAA) must be configured on the port for all network-related service requests. The authentication method list must be enabled and specified. A method list describes the sequence and authentication method to be queried to authenticate a user. See the IEEE 802.1X Authenticator feature module for information.
- The port must be successfully authenticated.

The IEEE 802.1X Port-Based Authentication feature is available only on Cisco 89x and 88x series integrated switching routers (ISRs) that support switch ports.

**Note** Optimal performance is obtained with a connection that has a maximum of eight hosts per port.

The following Cisco ISR-G2 routers are supported:

- 1900
- 2900
- 3900
- 3900e

The following cards or modules support switch ports:

- Enhanced High-speed WAN interface cards (EHWICs) with ACL support:
  - EHWIC-4ESG-P
  - EHWIC-9ESG-P
  - EHWIC-4ESG
  - EHWIC-9ESG

- High-speed WAN interface cards (HWICs) without ACL support:
  - HWIC-4ESW-P
  - HWIC-9ESW-P
  - HWIC-4ESW
  - HWIC-9ES

**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.

# Restrictions for IEEE 802.1X Port-Based Authentication

## IEEE 802.1X Port-Based Authentication Configuration Restrictions

- The IEEE 802.1X Port-Based Authentication feature is available only on a switch port.
- 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.
- When IEEE 802.1X authentication is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- Changes to a VLAN to which an IEEE 802.1X-enabled port is assigned are transparent and do not affect the switch port. For example, a change occurs if a port is assigned to a RADIUS server-assigned VLAN and is then assigned to a different VLAN after reauthentication.
- When IEEE 802.1X authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- This feature does not support standard ACLs on the switch port.
- The IEEE 802.1X protocol is supported only on Layer 2 static-access ports, Layer 2 static-trunk ports, voice VLAN-enabled ports, and Layer 3 routed ports.

**Note** Ethernet interfaces can be configured either as access ports or as trunk ports with the following specifications:

- An access port can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.
- A trunk port can have two or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously.

- The IEEE 802.1X protocol is not supported on the following 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.

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

- Configuring the same VLAN ID for both access and voice traffic (using the **switchport access vlan** *vlan-id* and the **switchport voice vlan** *vlan-id* commands) fails if authentication has already been configured on the port.
- Configuring authentication on a port on which you have already configured **switchport access vlan** *vlan-id* and **switchport voice vlan** *vlan-id* fails if the access VLAN and voice VLAN have been configured with the same VLAN ID.

# 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.

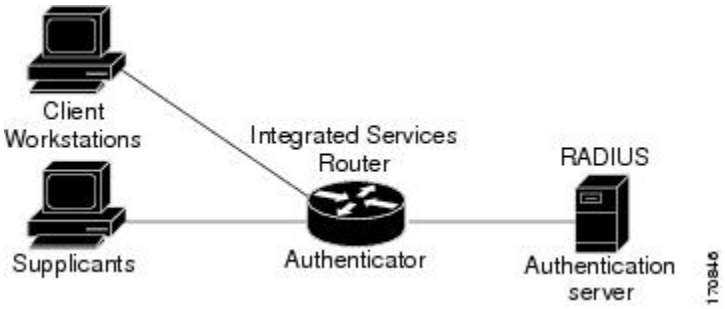
**Note** To ensure that information about any IEEE 802.1x-related commands that is entered on a port is automaticallly added to the running configuration to address any backward compatibility issues, use the **dot1x pae authenticator** command.

# Information About IEEE 802.1X Port-Based Authentication

## IEEE 802.1X Device Roles

With IEEE 802.1X authentication, the devices in the network have specific roles as shown in the figure below.

***Figure 1: IEEE 802.1X Device Roles***




- 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.

# IEEE 802.1X 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 **authentication 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.

**Note** Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1xport-control** command.

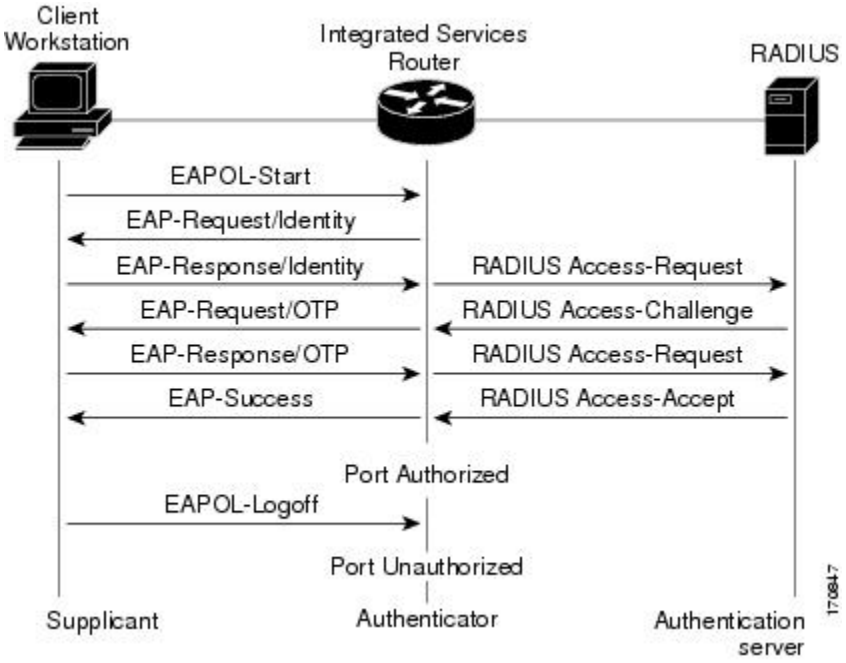
However, if during bootup the supplicant does not receive an EAP-request/identity frame from the router, the supplicant can initiate authentication by sending an EAPOL-start frame, which prompts the router to request the supplicant's identity.

**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: Message Exchange***




# IEEE 802.1X 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), this event occurs:

- 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 this situation 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-name interface-number* privileged EXEC command.

# IEEE 802.1X Host Mode

You can configure an IEEE 802.1X port for single-host or for multihost 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 multihost 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.

# IEEE 802.1X Port Authorization 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, Cisco Discovery Protocol (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, then 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.

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.

# IEEE 802.1X—Conditional Logging

Use the IEEE 802.1X—Conditional Logging feature for troubleshooting. When the Conditional Logging feature is enabled, the router generates debugging messages for packets entering or leaving the router on a specified interface; the router will not generate debugging output for packets entering or leaving through a different interface. You can specify the interfaces explicitly. For example, you may want to see only debugging messages for one interface or subinterface. You can also turn on debugging for all interfaces that meet the configured condition. This feature is useful on dial access servers, which have a large number of ports.

Normally, the router will generate debugging messages for every interface, resulting in a large number of messages. The large number of messages consumes system resources, and can affect your ability to find the specific information you need. By limiting the number of debugging messages, you can receive messages related to only the ports you want to troubleshoot.

For more information on conditional logging and enabling conditionally triggered debugging, see the "Enabling Conditionally Triggered Debugging" section of the "Troubleshooting and Fault Management" chapter in the *Basic System Management Configuration Guide*.

# 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)

# How to Configure IEEE 802.1X Port-Based Authentication

## Enabling IEEE 802.1X Authentication and Authorization

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*]
5. **dot1x system-auth-control**
6. **identity profile default**
7. **interface** *type slot/port*
8. **authentication port-control** {**auto** | **force-authorized** | **force-unauthorized**}
9. **dot1x pae** [**supplicant** | **authenticator** | **both**]
10. **end**
11. **show dot1x**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Device(config)# aaa new-model` | Enables AAA. |
| **Step 4** | **aaa authentication dot1x** {**default** \| *listname*} *method1* [*method2...*]<br><br>**Example:**<br>`Device(config)# aaa authentication dot1x default group radius` | Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **dot1x system-auth-control**<br><br>**Example:**<br>`Device(config)# dot1x system-auth-control` | Globally enables 802.1X port-based authentication. |
| **Step 6** | **identity profile default**<br><br>**Example:**<br>`Device(config)# identity profile default` | Creates an identity profile and enters dot1x profile configuration mode. |
| **Step 7** | **interface** *type slot/port*<br><br>**Example:**<br>`Device(config-identity-prof)# interface fastethernet 0/1` | Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication. |
| **Step 8** | **authentication port-control** {**auto** \| **force-authorized** \| **force-unauthorized**}<br><br>**Example:**<br>`Device(config-if)# authentication port-control auto` | Enables 802.1X port-based authentication on the interface.<br>• **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.<br>• **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.<br>• **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.<br><br>**Note** Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1xport-control** command. |
| **Step 9** | **dot1x pae** [**supplicant** \| **authenticator** \| **both**]<br><br>**Example:**<br>`Device(config-if)# dot1x pae authenticator` | Sets the Port Access Entity (PAE) type.<br>• **supplicant—**The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator.<br>• **authenticator-—**The interface acts only as an authenticator and does not respond to any messages meant for a supplicant. |

| | Command or Action | Purpose |
|---|---|---|
| | | • **both—**The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages. |
| **Step 10** | **end**<br><br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and enters privileged EXEC mode. |
| **Step 11** | **show dot1x**<br><br>**Example:**<br>`Device# show dot1x` | Displays whether 802.1X authentication has been configured on the device. |

# Configuring the IEEE 802.1X Host Mode

**Note** This section describes IEEE 802.1X security features available only on the switch ports.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *type number*
5. **authentication host-mode** {**multi-auth** | **multi-domain** | **multi-host** | **single-host**} [**open**]
6. **switchport voice vlan** *vlan-id*
7. **end**
8. **show authentication interface** *type number*
9. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **radius-server vsa send authentication**<br><br>**Example:**<br>`Device(config)# radius-server vsa send authentication` | Configures the Network Access Server (NAS) to recognize and use vendor-specific attributes. |
| **Step 4** | **interface** *type number*<br><br>**Example:**<br>`Device(config)# interface fastethernet 2/1` | Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode. |
| **Step 5** | **authentication host-mode** {**multi-auth** \| **multi-domain** \| **multi-host** \| **single-host**} [**open**]<br><br>**Example:**<br>`Device(config-if)# authentication host-mode single-host fastethernet 2/1` | Allows a single host (client) or multiple hosts on the 802.1X-authorized port.<br>• The **multi-auth** keyword specifies multiple authentications to occur on the 802.1X-authorized port.<br>• The **multi-domain** keyword specifies multi-domain authentication (MDA), which is used to enable authentication of both a host and a voice device, such as an IP phone (Cisco or non-Cisco) on the same switch port.<br>• The **multi-host** keyword specifies multiple hosts on the 802.1X-authorized port.<br>• The **single-host** keyword specifies a single client on the 802.1X-authorized port.<br>• (Optional) The **open** keyword specifies that the port is open; that is, there are no access restrictions. |
| **Step 6** | **switchport voice vlan** *vlan-id*<br><br>**Example:**<br>`Device(config-if)# switchport voice vlan 2` | (Optional) Configures the voice VLAN. |
| **Step 7** | **end**<br><br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |
| **Step 8** | **show authentication interface** *type number*<br><br>**Example:**<br>`Device# show authentication interface` | Displays your entries. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **copy running-config startup-config**<br><br>**Example:**<br>`Device# copy running-config startup-config` | Saves your entries in the configuration file. |

# Enabling IEEE 802.1X SNMP Notifications on Switch Ports

## 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 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. |

# Configuration Examples for IEEE 802.1x Port-Based Authentication

## Example: Enabling IEEE 802.1X and AAA on a Port

**Note** Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1xport-control** command.

**Note** Whenever you configure any IEEE 802.1X parameter on a port, a dot1x authenticator is automatically created on the port. As a result, the **dot1x pae authenticator** command 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.

The following example shows how to enable IEEE 802.1X and AAA on Fast Ethernet port 2/1 and how to verify the configuration:

**Note** In this example the Ethernet interface is configured as an access port by using the **switchport mode access** command in interface configuration mode. The Ethernet interface can also be configured as a trunk port using the **switchport mode trunk** command in interface configuration mode.

```
Device> enable
Device# configure terminal
Device(config)# dot1x system-auth-control
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# interface fastethernet2/1
Device(config-if)# switchport mode access
Device(config-if)# authentication port-control auto
Device(config-if)# dot1x pae authenticator
Device(config-if)# end

Device# 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
```

# Example: Configuring the IEEE 802.1X Host Mode

The following example shows how to enable 802.1X authentication and to allow multiple hosts:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication port-control auto
Device(config-if)# authentication host-mode multihost
Device(config-if)# end
```

# Example: Displaying IEEE 802.1X Statistics and Status

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

The following example displays **show dot1x all** command output:

```
Device# 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#
```

The following example displays **show dot1x summary** command output:

```
Device# show dot1x all summary

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

# AdditionalReferencesforIEEE802.1XPort-BasedAuthentication

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| IEEE 802.1X | *Port Based Network Access Control* |
| RFC 3580 | *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* |

### MIBs

| MIB | MIBs Link |
|---|---|
| • Cisco-PAE-MIB<br>• IEEE8021-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 |

### 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 IEEE 802.1X Port-Based Authentication

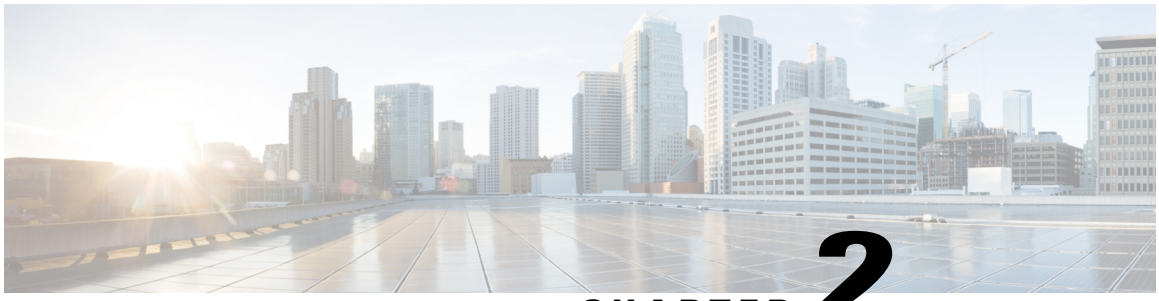
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 1: Feature Information for IEEE 802.1X Port-Based Authentication***

| Feature Name | Releases | Feature Information |
|---|---|---|
| CDP Enhancement —Host Presence TLV | | This features allows you to ensure that 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. |
| IEEE 802.1X Authenticator | | This feature was introduced to prevent unauthorized devices (supplicants) from gaining access to the network.<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-Conditional Logging | | The IEEE 802.1X-Conditional Logging feature is used for troubleshooting interfaces. |
| IEEE 802.1X MIB Support | | This feature provides support for the following MIBs:<br>• Cisco-PAE-MIB<br>• IEEE8021-PAE-MIB |
| IEEE 802.1X Support for Trunk Ports | | The IEEE 802.1X Support for Trunk Ports feature is used to configure Ethernet interfaces as trunk ports. |



CHAPTER 2

# IEEE 802.1X Common Session ID

The IEEE 802.1X Common Session ID feature allows a single session identifier to be used for all 802.1X and MAB authenticated sessions. This session ID is used for all reporting purposes such as show commands, MIBs, and RADIUS messages and allows users to distinguish messages for one session from messages for other sessions.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 IEEE 802.1X Common Session ID

The following tasks must be completed before implementing the IEEE 802.1X Common Session ID feature:

- IEEE 802.1X must be enabled on the device port.

- The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs).
- EAP support must be enabled on the RADIUS server.
- 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.
- Authentication, authorization, and accounting (AAA) must be configured on the port for all network-related service requests. The authentication method list must be enabled and specified. A method list describes the sequence and authentication method to be queried to authenticate a user. See the IEEE 802.1X Authenticator feature module for information.
- The port must be successfully authenticated.

The IEEE 802.1X Common Session ID feature is available only on Cisco 89x and 88x series integrated switching routers (ISRs) that support switch ports.

The following ISR-G2 routers are supported:

- 1900
- 2900
- 3900
- 3900e

The following cards or modules support switch ports:

- Enhanced High-speed WAN interface cards (EHWICs) with ACL support:
  - EHWIC-4ESG-P
  - EHWIC-9ESG-P
  - EHWIC-4ESG
  - EHWIC-9ESG
- High-speed WAN interface cards (HWICs) without ACL support:
  - HWIC-4ESW-P
  - HWIC-9ESW-P
  - HWIC-4ESW
  - HWIC-9ES

**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, use the **show interfaces switchport** command.

# Restrictions for IEEE 802.1X Common Session ID

- The IEEE 802.1X Common Session ID feature is available only on a switch port.
- This feature does not support standard ACLs on the switch port.

# Information About IEEE 802.1X Common Session ID

## IEEE 802.1X Common Session ID Reporting

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

The session ID includes:

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

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

# Examples for IEEE 802.1X Common Session ID

## Example: Common Session ID in Authentication Session Output

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

```
Switch# show authentication sessions

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

## Example: Common Session ID in Syslog Output

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

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

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

# AdditionalReferencesforIEEE802.1XPort-BasedAuthentication

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| IEEE 802.1X | *Port Based Network Access Control* |
| RFC 3580 | *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* |

### MIBs

| MIB | MIBs Link |
|---|---|
| • Cisco-PAE-MIB<br>• IEEE8021-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 |

### 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 |

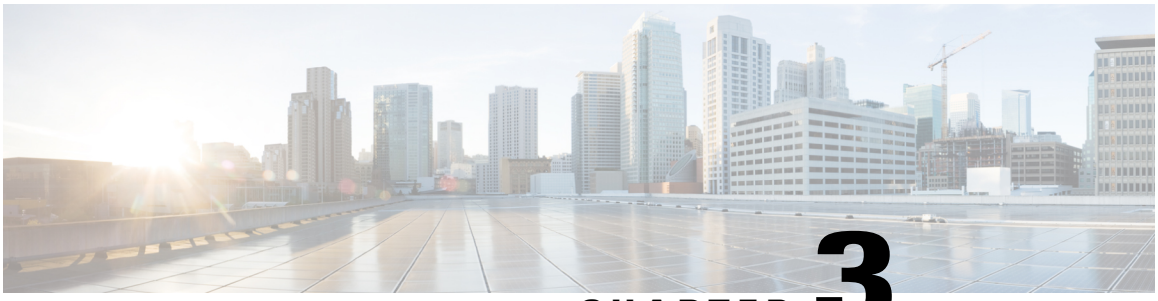
# Feature Information for IEEE 802.1X Common Session ID

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 2: Feature Information for IEEE 802.1X Common Session ID***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE 802.1X Common Session ID | | The IEEE 802.1X Common Session ID feature allows a single session identifier to be used for all 802.1X and MAB authenticated sessions. This session ID is used for all reporting purposes such as show commands, MIBs, and RADIUS messages and allows users to distinguish messages for one session from messages for other sessions. |



CHAPTER 3

# IEEE 802.1X Guest VLAN

The IEEE 802.1X Guest VLAN feature allows a guest VLAN to be configured for each 802.1X port on the device to provide limited services to non-802.1X-compliant clients.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 IEEE 802.1X Guest VLAN

The following tasks must be completed before implementing the IEEE 802.1X Guest VLAN feature:

- IEEE 802.1X must be enabled on the device port.
- The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs).

- EAP support must be enabled on the RADIUS server.
- 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.
- Authentication, authorization, and accounting (AAA) must be configured on the port for all network-related service requests. The authentication method list must be enabled and specified. A method list describes the sequence and authentication method to be queried to authenticate a user. See the IEEE 802.1X Authenticator feature module for information.
- The port must be successfully authenticated.

The IEEE 802.1X Guest VLAN Support feature is available only on Cisco 89x and 88x series integrated switching routers (ISRs) that support switch ports.

The following ISR-G2 routers are supported:

- 1900
- 2900
- 3900
- 3900e

The following cards or modules support switch ports:

- Enhanced High-speed WAN interface cards (EHWICs) with ACL support:
  - EHWIC-4ESG-P
  - EHWIC-9ESG-P
  - EHWIC-4ESG
  - EHWIC-9ESG
- High-speed WAN interface cards (HWICs) without ACL support:
  - HWIC-4ESW-P
  - HWIC-9ESW-P
  - HWIC-4ESW
  - HWIC-9ES

**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, use the **show interfaces switchport** command.

# Restrictions for IEEE 802.1X Guest VLAN

- The IEEE 802.1X Guest VLAN feature is available only on a switch port.
- 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.
- When IEEE 802.1X authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- This feature does not support standard ACLs on the switch port.

# Information About IEEE 802.1X Guest VLAN

## IEEE 802.1X Authentication with Guest VLAN

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 to access 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.

**Note** Guest VLANs are supported on IEEE 802.1X ports in single-host or multihost mode.

# How to Configure IEEE 802.1X Guest VLAN

## Configuring IEEE 802.1X Guest VLAN

When you configure a guest VLAN, clients that are not 802.1X-capable are put into the guest VLAN when the server does not receive a response to its EAP-request/identity frame. Clients that are 802.1X-capable but that fail authentication are not granted network access. The switch supports guest VLANs in single-host, multiple-host and multidomain modes. The switch does not support guest VLANs in multiauth mode.

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

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

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **authentication port-control auto**
4. **exit**
5. **dot1x guest-vlan supplicant**
6. **end**
7. **show authentication interface** *interface-id*
8. **copy running-config startup-config**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **interface** *type slot/port*<br>**Example:**<br>`Switch(config)# interface gigabitethernet0/1` | Specifies the port to be configured, and enters interface configuration mode.<br>• For the supported port types, see the "802.1x Authentication Configuration Guidelines" section of the "Configuring IEEE 1802.1X Port-Based Authentication" module. |
| **Step 3** | **authentication port-control auto**<br>**Example:**<br>`Switch(config-if)# authentication port-control auto` | Enables 802.1X authentication on the port. |
| **Step 4** | **exit**<br>**Example:**<br>`Switch(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 5** | **dot1x guest-vlan supplicant**<br>**Example:**<br>`Switch(config)# dot1x guest-vlan supplicant` | Specifies the supplicant as an 802.1X guest VLAN.<br>• You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1X guest VLAN. |
| **Step 6** | **end**<br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show authentication interface** *interface-id*<br>**Example:**<br>`Switch# show authentication interface gigabitethernet0/1` | Verifies your entries. |
| **Step 8** | **copy running-config startup-config**<br>**Example:**<br>`Switch# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuration Examples for IEEE 802.1X Guest VLAN

## Example Configuring IEEE 802.1X Guest VLAN

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

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# authentication port-control auto
Switch(config-if)# exit
Switch(config)# dot1x guest-vlan supplicant
```

# AdditionalReferencesforIEEE802.1XPort-BasedAuthentication

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| IEEE 802.1X | *Port Based Network Access Control* |
| RFC 3580 | *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* |

### MIBs

| MIB | MIBs Link |
|---|---|
| • Cisco-PAE-MIB<br>• IEEE8021-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 |

### 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 |

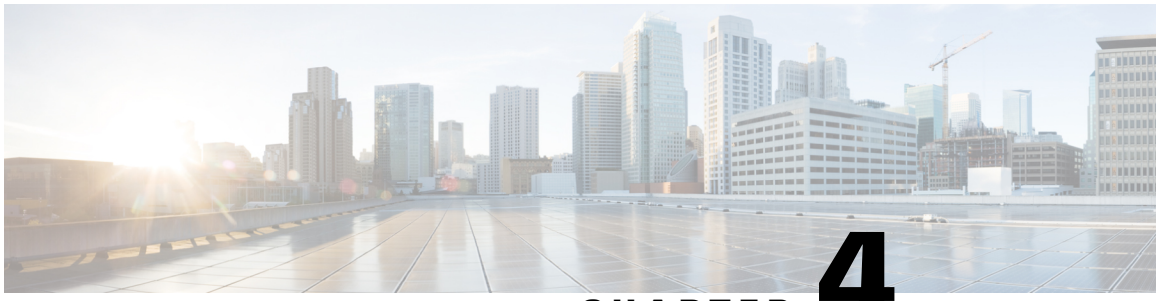
# Feature Information for IEEE 802.1X Guest VLAN

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 IEEE 802.1X Guest VLAN***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE 802.1X Guest VLAN | | The IEEE 802.1X Guest VLAN feature allows a guest VLAN to be configured for each 802.1X port on the device to provide limited services to non-802.1X-compliant clients. |



CHAPTER 4

# IEEE 802.1X RADIUS Accounting

The IEEE 802.1X RADIUS Accounting feature is used to relay important events to the RADIUS server (such as the supplicant's connection session). The information in these events is used for security and billing purposes.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 RADIUS Accounting

The following tasks must be completed before implementing the IEEE 802.1X RADIUS Accounting feature:

- IEEE 802.1X must be enabled on the device port.

- The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs).
- EAP support must be enabled on the RADIUS server.
- 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.
- Authentication, authorization, and accounting (AAA) must be configured on the port for all network-related service requests. The authentication method list must be enabled and specified. A method list describes the sequence and authentication method to be queried to authenticate a user. See the IEEE 802.1X Authenticator feature module for information.
- The port must be successfully authenticated.
- If you plan to implement system-wide accounting, you should also configure IEEE 802.1X accounting. You also 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.

The RADIUS Accounting feature is available only on Cisco 89x and 88x series integrated switching routers (ISRs) that support switch ports.

The following ISR-G2 routers are supported:

- 1900
- 2900
- 3900
- 3900e

The following cards or modules support switch ports:

- Enhanced High-speed WAN interface cards (EHWICs) with ACL support:
  - EHWIC-4ESG-P
  - EHWIC-9ESG-P
  - EHWIC-4ESG
  - EHWIC-9ESG
- High-speed WAN interface cards (HWICs) without ACL support:
  - HWIC-4ESW-P
  - HWIC-9ESW-P
  - HWIC-4ESW
  - HWIC-9ES

**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.

# Restrictions for IEEE 802.1X with RADIUS Accounting

- The IEEE 802.1X with RADIUS Accounting feature is available only on a switch port.
- This feature does not support standard ACLs on the switch port.

# Information About IEEE 802.1X with RADIUS Accounting

## Relaying of IEEE 802.1X RADIUS Accounting Events

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.

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.

The following 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 perform the following tasks:

**Note** See the "Enabling 802.1X Accounting" section for more specific configuration information.

- Enable accounting in your RADIUS server.
- Enable IEEE 802.1X accounting on your switch.
- Enable AAA accounting.

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 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.

# 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.

**Note** The Framed-IP-Address AV pair (Attribute 8) is sent only if a valid Dynamic Host Control Protocol (DHCP) binding exists for the host in the DHCP snooping bindings table.

**Note** With CSCtz66183, the Service-Type AV pair (Attribute 6) is not displayed in the Accounting-Request records.

***Table 4: 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 | Sometimes 1 |
| Attribute [25] | Class | Always | Always | Always |
| Attribute [30] | Called-Station-ID | Always | Always | Always |
| Attribute [31] | Calling-Station-ID | Always | Always | Always |
| Attribute [40] | Acct-Status-Type | Always | Always | Always |
| Attribute [41] | Acct-Delay-Time | Always | Always | Always |
| Attribute [42] | Acct-Input-Octets | Never | Always | Always |
| Attribute [43] | Acct-Output-Octets | Never | Always | Always |
| Attribute [44] | Acct-Session-ID | Always | Always | Always |
| Attribute [45] | Acct-Authentic | Always | Always | Always |
| Attribute [46] | Acct-Session-Time | Never | Never | Always |
| Attribute [47] | Acct-Input-Packets | Never | Always | Always |

| Attribute Number | AV Pair Name | *START* | *INTERIM* | *STOP* |
|---|---|---|---|---|
| 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 device to send Cisco vendor-specific attributes (VSAs) to the RADIUS server. The following table lists the available Cisco AV pairs.

**Note** Before VSAs can be sent in the accounting records you must configure the **radius-server vsa send accounting** command.

***Table 5: 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 display 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 Command Reference*. For more information about AV pairs, see Cisco IOS RFC 3580, *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*.

# How to Use IEEE 802.1X RADIUS Accounting

## Enabling 802.1X RADIUS Accounting

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **acct-port** *port-number*
5. **aaa accounting dot1x default start-stop group radius**
6. **aaa accounting system default start-stop group radius**
7. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Device(config)# aaa new-model` | Enables AAA globally. |
| **Step 4** | **radius-server host** {*hostname* \| *ip-address*} **auth-port** *port-number* **acct-port** *port-number*<br><br>**Example:**<br>\|<br>`Device(config)# radius-server host 172.20.39.46 auth-port 1812 acct-port 1813 key rad123` | Specifies a RADIUS server host.<br>• The **auth-port** keyword and *port-number* argument specifies the User Datagram Protocol (UDP) destination port for authentication requests.<br>• The **acct-port** keyword and *port-number* argument specifies the UDP destination port for accounting requests. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **aaa accounting dot1x default start-stop group radius**<br><br>**Example:**<br>`Device(config)# aaa accounting dot1x default start-stop group radius` | Provides information about all IEEE 802.1x-related user events.<br>• The **start-stop** keyword sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.<br>• The **group radius** is the exact name of the character string used to name the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command. |
| **Step 6** | **aaa accounting system default start-stop group radius**<br><br>**Example:**<br>`Device(config)# aaa accounting system default start-stop group radius` | Performs accounting for all system-level events not associated with users, such as reloads.<br>**Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.<br>• The **start-stop** keyword sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.<br>• The **group radius** is the exact name of the character string used to name the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command. |
| **Step 7** | **end**<br><br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and enters privileged EXEC mode. |

# Configuration Example for IEEE 802.1X RADIUS Accounting

## Example: Enabling IEEE 802.1X RADIUS Accounting

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 1812 as the authorization port, 1813 as the UDP port for accounting, and rad123 as the encryption key:

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

```
Router# configure terminal
Router(config)# aaa new-model
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#
```

# Additional References for IEEE 802.1X Port-Based Authentication

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| IEEE 802.1X | *Port Based Network Access Control* |
| RFC 3580 | *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* |

### MIBs

| MIB | MIBs Link |
|---|---|
| • Cisco-PAE-MIB<br>• IEEE8021-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 |

### 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 |

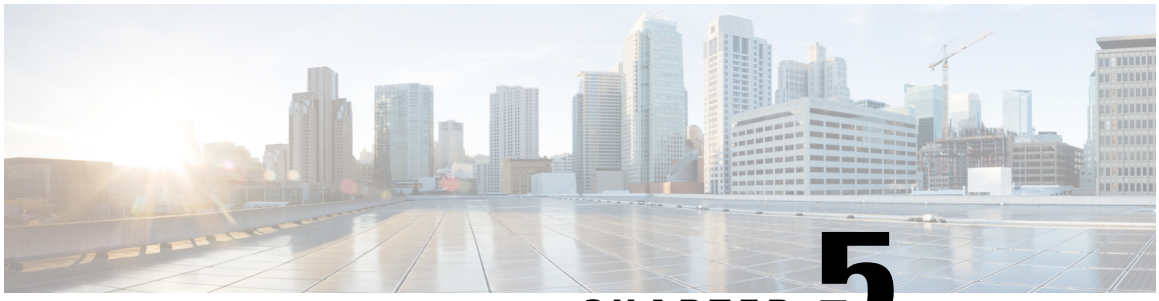
# Feature Information for IEEE 802.1X RADIUS Accounting

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 6: Feature Information for IEEE 802.1X RADIUS Accounting***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE 802.1X RADIUS Accounting | | This feature is used to relay important events to the RADIUS server (such as the supplicant's connection session). The information in these events is used for security and billing purposes. |



CHAPTER 5

# IEEE 802.1X VLAN Assignment

The IEEE 802.1X VLAN Assignment feature is automatically enabled when IEEE 802.1X authentication is configured for an access port, which allows the RADIUS server to send a VLAN assignment to the device port. This assignment configures the device port so that network access can be limited for certain users.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 IEEE 802.1X VLAN Assignment

The following tasks must be completed before implementing the IEEE 802.1X VLAN Assignment feature:

- IEEE 802.1X must be enabled on the device port.

- The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs).
- EAP support must be enabled on the RADIUS server.
- 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.
- Authentication, authorization, and accounting (AAA) must be configured on the port for all network-related service requests. The authentication method list must be enabled and specified. A method list describes the sequence and authentication method to be queried to authenticate a user. See the IEEE 802.1X Authenticator feature module for information.
- The port must be successfully authenticated.

The IEEE 802.1X VLAN Assignment feature is available only on Cisco 89x and 88x series integrated switching routers (ISRs) that support switch ports.

The following ISR-G2 routers are supported:

- 1900
- 2900
- 3900
- 3900e

The following cards or modules support switch ports:

- Enhanced High-speed WAN interface cards (EHWICs) with ACL support:
  - EHWIC-4ESG-P
  - EHWIC-9ESG-P
  - EHWIC-4ESG
  - EHWIC-9ESG
- High-speed WAN interface cards (HWICs) without ACL support:
  - HWIC-4ESW-P
  - HWIC-9ESW-P
  - HWIC-4ESW
  - HWIC-9ES

**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, use the **show interfaces switchport** command.

# Restrictions for IEEE 802.1X VLAN Assignment

- The IEEE 802.1X VLAN Assignment feature is available only on a switch port.
- The device 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
- When IEEE 802.1X authentication is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN.
- 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 multihost 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.
- This feature does not support standard ACLs on the switch port.

# Information About IEEE 802.1X VLAN Assignment

## Configuring Authorization

The AAA authorization feature is used to determine what a user can and cannot do. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either

in the local user database or on the security server, to configure the user's session. Once this is done, the user is granted access to a requested service only if the information in the user profile allows it.

## IEEE 802.1X Authentication with VLAN Assignment

In Cisco IOS Release 12.4(11)T and later releases, the device 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 device port.

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

# How to Configure IEEE 802.1X VLAN Assignment

## Enabling AAA Authorization for VLAN Assignment

AAA authorization limits the services available to a user. When AAA authorization is enabled, the device uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization network radius if-authenticated**
5. **aaa authorization exec radius if-authenticated**
6. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Device(config)# aaa new-model` | Enables AAA. |
| **Step 4** | **aaa authorization network radius if-authenticated**<br><br>**Example:**<br>`Device(config)# aaa authorization network radius if-authenticated` | Configures the device for user RADIUS authorization for all network-related service requests. RADIUS authorization succeeds if the user has authenticated. |
| **Step 5** | **aaa authorization exec radius if-authenticated**<br><br>**Example:**<br>`Device(config)# aaa authorization exec radius if-authenticated` | Configures the device for user RADIUS authorization if the user has privileged EXEC access. RADIUS authorization succeeds if the user has authenticated. |
| **Step 6** | **end**<br><br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and enters privileged EXEC mode. |

# Enabling IEEE 802.1X Authentication and Authorization

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*]
5. **dot1x system-auth-control**
6. **identity profile default**
7. **interface** *type slot/port*
8. **authentication port-control** {**auto** | **force-authorized** | **force-unauthorized**}
9. **dot1x pae** [**supplicant** | **authenticator** | **both**]
10. **end**
11. **show dot1x**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Device(config)# aaa new-model` | Enables AAA. |
| **Step 4** | **aaa authentication dot1x** {**default** \| *listname*} *method1* [*method2...*]<br><br>**Example:**<br>`Device(config)# aaa authentication dot1x default group radius` | Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server. |
| **Step 5** | **dot1x system-auth-control**<br><br>**Example:**<br>`Device(config)# dot1x system-auth-control` | Globally enables 802.1X port-based authentication. |
| **Step 6** | **identity profile default**<br><br>**Example:**<br>`Device(config)# identity profile default` | Creates an identity profile and enters dot1x profile configuration mode. |
| **Step 7** | **interface** *type slot/port*<br><br>**Example:**<br>`Device(config-identity-prof)# interface fastethernet 0/1` | Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication. |
| **Step 8** | **authentication port-control** {**auto** \| **force-authorized** \| **force-unauthorized**}<br><br>**Example:**<br>`Device(config-if)# authentication port-control auto` | Enables 802.1X port-based authentication on the interface.<br>• **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 |

| | Command or Action | Purpose |
|---|---|---|
| | | attempting to access the network is uniquely identified by the router by using the supplicant MAC address.<br>• **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.<br>• **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.<br>**Note** Effective with Cisco IOS Release 12.2(33)SXI, the **authentication port-control** command replaces the **dot1xport-control** command. |
| **Step 9** | **dot1x pae** [**supplicant** \| **authenticator** \| **both**]<br>**Example:**<br>`Device(config-if)# dot1x pae authenticator` | Sets the Port Access Entity (PAE) type.<br>• **supplicant—**The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator.<br>• **authenticator**-—The interface acts only as an authenticator and does not respond to any messages meant for a supplicant.<br>• **both—**The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages. |
| **Step 10** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and enters privileged EXEC mode. |
| **Step 11** | **show dot1x**<br>**Example:**<br>`Device# show dot1x` | Displays whether 802.1X authentication has been configured on the device. |

# Specifying an Authorized VLAN in the RADIUS Server Database

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the device and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification.

- You must assign the following vendor-specific tunnel attributes in the RADIUS server database. The RADIUS server must return these attributes to the device:

- [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.

# Configuration Example for IEEE 802.1X VLAN Assignment

## Example: Enabling AAA Authorization for VLAN Assignment

The following example shows how to enable AAA Authorization for VLAN assignment:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization network radius if-authenticated
Device(config)# aaa authorization exec radius if-authenticated
Device(config)# end
```

## Example: Enabling 802.1X Authentication

The following example shows how to enable 802.1X authentication on a device:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius group radius
Device(config)# dot1x system-auth-control
Device(config)# interface fastethernet 1
Device(config-if)# dot1x port-control auto
```

The following **show dot1x** command output shows that 802.1X authentication has been configured on a device:

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Enabled
QuietPeriod               = 600
ServerTimeout             = 60
SuppTimeout               = 30
ReAuthPeriod              = 1800 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 3
TxPeriod                  = 60
RateLimitPeriod           = 60
```

# Example: Specifying an Authorized VLAN in the RADIUS Server Database

This example shows how to specify an authorized VLAN in the RADIUS server by assigning vendor-specific tunnel attributes:

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

# Additional References for IEEE 802.1X Port-Based Authentication

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| IEEE 802.1X | *Port Based Network Access Control* |
| RFC 3580 | *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* |

### MIBs

| MIB | MIBs Link |
|---|---|
| • Cisco-PAE-MIB<br>• IEEE8021-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 |

### 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 |

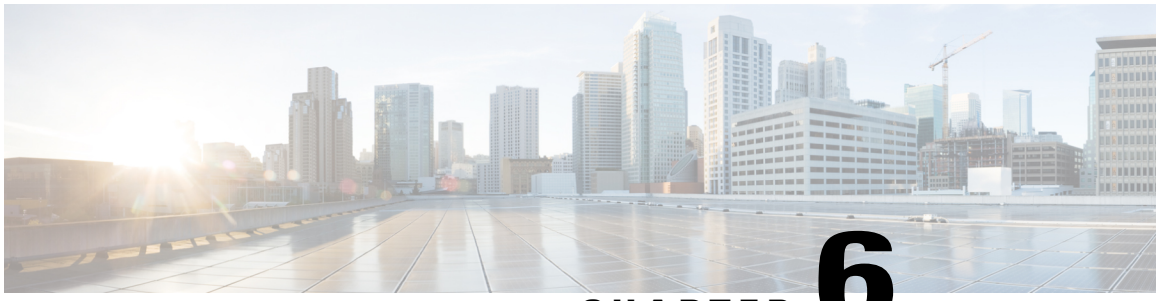
# Feature Information for IEEE 802.1X VLAN Assignment

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 7: Feature Information for IEEE 802.1X VLAN Assignment***

| Feature Name | Releases | Feature Information |
|---|---|---|
| IEEE Information for IEEE 802.1X VLAN Assignment | | The IEEE 802.1X VLAN Assignment feature is automatically enabled when IEEE 802.1X authentication is configured for an access port, which allows the RADIUS server to send a VLAN assignment to the device port. This assignment configures the device port so that network access can be limited for certain users. |



CHAPTER 6

# RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy.



# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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.

# Information About RADIUS Change of Authorization

## About RADIUS Change of Authorization

A standard RADIUS interface is typically used in a pulled model, in which the request originates from a device attached to a network and the response is sent from the queried servers. The Cisco software supports the RADIUS CoA request defined in RFC 5176 that is used in a pushed model, in which the request originates

from the external server to the device attached to the network, and enables the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

Use the following per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce
- Security and Password
- Accounting

## CoA Requests

CoA requests, as described in RFC 5176, are used in a pushed model to allow for session identification, host reauthentication, and session termination. The model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the device that acts as a listener.

### RFC 5176 Compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the device for a session termination.

The following table shows the IETF attributes that are supported for the RADIUS Change of Authorization (CoA) feature.

***Table 8: Supported IETF Attributes***

| Attribute Number | Attribute Name |
|---|---|
| 24 | State |
| 31 | Calling-Station-ID |
| 44 | Acct-Session-ID |
| 80 | Message-Authenticator |
| 101 | Error-Cause |

The following table shows the possible values for the Error-Cause attribute.

*Table 9: Error-Cause Values*

| Value | Explanation |
|---|---|
| 201 | Residual Session Context Removed |
| 202 | Invalid EAP Packet (Ignored) |
| 401 | Unsupported Attribute |
| 402 | Missing Attribute |
| 403 | NAS Identification Mismatch |
| 404 | Invalid Request |
| 405 | Unsupported Service |
| 406 | Unsupported Extension |
| 407 | Invalid Attribute Value |
| 501 | Administratively Prohibited |
| 502 | Request Not Routable (Proxy) |
| 503 | Session Context Not Found |
| 504 | Session Context Not Removable |
| 505 | Other Proxy Processing Error |
| 506 | Resources Unavailable |
| 507 | Request Initiated |
| 508 | Multiple Session Selection Unsupported |

## CoA Request Response Code

The CoA Request Response code can be used to issue a command to the device. The supported commands are listed in the “CoA Request Commands” section.

The packet format for a CoA Request Response code as defined in RFC 5176 consists of the following fields: Code, Identifier, Length, Authenticator, and Attributes in the Type:Length:Value (TLV) format.

The Attributes field is used to carry Cisco VSAs.

### Session Identification

For disconnect and CoA requests targeted at a particular session, the device locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco vendor-specific attribute (VSA))
- Calling-Station-Id (IETF attribute #31, which contains the host MAC address)

Unless all session identification attributes included in the CoA message match the session, the device returns a Disconnect-NAK or CoA-NAK with the "Invalid Attribute Value" error-code attribute.

**Note** A CoA NAK message is not sent for all CoA requests with a key mismatch. The message is sent only for the first three requests for a client. After that, all the packets from that client are dropped. When there is a key mismatch, the response authenticator sent with the CoA NAK message is calculated from a dummy key value.

### CoA ACK Response Code

If an authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within a CoA ACK can vary based on the CoA Request.

### CoA NAK Response Code

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure.

## CoA Request Commands

The commands supported on the device are shown in the table below. All CoA commands must include the session identifier between the device and the CoA client.

***Table 10: CoA Request Commands Supported on the Device***

| Command | Cisco VSA |
|---|---|
| Bounce host port | Cisco:Avpair="subscriber:command=bounce-host-port" |
| Disable host port | Cisco:Avpair="subscriber:command=disable-host-port" |
| Reauthenticate host | Cisco:Avpair="subscriber:command=reauthenticate" |
| Terminate session | This is a standard disconnect request that does not require a VSA |

### Session Reauthentication

To initiate session reauthentication, the authentication, authorization, and accounting (AAA) server sends a standard CoA-Request message that contains a Cisco VSA and one or more session identification attributes. The Cisco VSA is in the form of Cisco:Avpair="subscriber:command=reauthenticate".

The current session state determines the device's response to the message in the following scenarios:

- If the session is currently authenticated by IEEE 802.1*x*, the device responds by sending an Extensible Authentication Protocol over LAN (EAPoL)-RequestId message to the server.
- If the session is currently authenticated by MAC authentication bypass (MAB), the device sends an access request to the server, passing the same identity attributes used for the initial successful authentication.
- If session authentication is in progress when the device receives the command, the device terminates the process and restarts the authentication sequence, starting with the method configured to be attempted first.

### Session Termination

A CoA Disconnect-Request terminates the session without disabling the host port. CoA Disconnect-Request termination causes reinitialization of the authenticator state machine for the specified host, but does not restrict the host's access to the network. If the session cannot be located, the device returns a Disconnect-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device terminates the session. After the session has been completely removed, the device returns a Disconnect-ACK message.

To restrict a host's access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism.

### CoA Request Disable Host Port

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism. This command is carried in a standard CoA-Request message that has the following VSA:

Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the "Session Identification" section. If the device cannot locate the session, it returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the device locates the session, it disables the hosting port and returns a CoA-ACK message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

To ignore the RADIUS server CoA disable port command, see the "Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests" section.

### CoA Request Bounce Port

A RADIUS server CoA bounce port sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the following VSA:

Cisco:Avpair="subscriber:command=bounce-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the Session Identification. If the session cannot be located, the device returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device disables the hosting port for a period of 10 seconds, reenables it (port-bounce), and returns a CoA-ACK.

To ignore the RADIUS server CoA bounce port, see the "Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests" section.

# How to Configure RADIUS Change of Authorization

## Configuring RADIUS Change of Authorization

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string*
6. **port** *port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Device(config)# aaa new-model` | Enables authentication, authorization, and accounting (AAA) globally. |
| **Step 4** | **aaa server radius dynamic-author**<br><br>**Example:**<br>`Device(config)# aaa server radius dynamic-author` | Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests. Configures the device as a AAA server to facilitate interaction with an external policy server. |
| **Step 5** | **client** {*ip-address* \| *name* [**vrf** *vrf-name*]} **server-key** [**0** \| **7**] *string*<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# client 10.0.0.1` | Configures the RADIUS key to be shared between a device and RADIUS clients. |
| **Step 6** | **port** *port-number*<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# port 3799` | Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients.<br><br>**Note** The default port for packet of disconnect is 1700. Port 3799 is required to interoperate with ACS 5.1. |
| **Step 7** | **auth-type** {**any** \| **all** \| **session-key**}<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# auth-type all` | Specifies the type of authorization that the device must use for RADIUS clients. The client must match the configured attributes for authorization. |
| **Step 8** | **ignore session-key**<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# ignore session-key` | (Optional) Configures the device to ignore the session key. |
| **Step 9** | **ignore server-key**<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# ignore server-key` | (Optional) Configures the device to ignore the server key. |
| **Step 10** | **exit**<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# exit` | Returns to global configuration mode. |

# Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests

When an authentication port is authenticated with multiple hosts and there is a Change of Authorization (CoA) request for one host to flap on this port or one host session to be terminated on this port, the other hosts on this port are also affected. Thus, an authenticated port with multiple hosts can trigger a DHCP renegotiation from one or more hosts in the case of a flap, or it can administratively shut down the authentication port that is hosting the session for one or more hosts.

Perform the following steps to configure the device to ignore RADIUS server Change of Authorization (CoA) requests in the form of a bounce port command or disable port command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **authentication command bounce-port ignore**
5. **authentication command disable-port ignore**
6. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Device(config)# aaa new-model` | Enables authentication, authorization, and accounting (AAA) globally. |
| **Step 4** | **authentication command bounce-port ignore**<br><br>**Example:**<br>`Device(config)# authentication command bounce-port ignore` | (Optional) Configures the device to ignore a RADIUS server bounce port command that causes a host to link flap on an authentication port, which causes DHCP renegotiation from one or more hosts connected to this port. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **authentication command disable-port ignore**<br><br>**Example:**<br>`Device(config)# authentication command disable-port ignore` | (Optional) Configures the device to ignore a RADIUS server CoA disable port command that administratively shuts down the authentication port that hosts one or more host sessions.<br>• The shutting down of the port causes session termination. |
| **Step 6** | **end**<br><br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

# Configuring the Dynamic Authorization Service for RADIUS CoA

Perform the following steps to enable the device as an authentication, authorization, and accounting (AAA) server for the dynamic authorization service. This service supports the Change of Authorization (CoA) functionality that pushes the policy map in an input and output direction.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
7. **port** *port-num*
8. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **aaa new-model**<br><br>**Example:**<br>`Device(config)# aaa new-model` | Enables AAA globally. |
| **Step 4** | **aaa server radius dynamic-author**<br><br>**Example:**<br>`Device(config)# aaa server radius dynamic-author` | Sets up the local AAA server for the dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction, and enters dynamic authorization local server configuration mode.<br>• In this mode, the RADIUS application commands are configured. |
| **Step 5** | **client** {*ip-addr* \| *hostname*} [**server-key** [**0** \| **7**] *string*]<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1` | Configures the IP address or hostname of the AAA server client.<br>• Use the optional **server-key** keyword and *string* argument to configure the server key at the client level.<br><br>**Note** Configuring the server key at the client level overrides the server key configured at the global level. |
| **Step 6** | **domain** {**delimiter** *character* \| **stripping** \| [**right-to-left**]}<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# domain stripping right-to-left` | (Optional) Configures username domain options for the RADIUS application.<br>• The **delimiter** keyword specifies the domain delimiter. One of the following options can be specified for the *character* argument: **@**, /, **$**, **%**, \, **#**, or **-**.<br>• The **stripping** keyword compares the incoming username with the names oriented to the left of the **@** domain delimiter.<br>• The **right-to-left** keyword terminates the string at the first delimiter going from right to left. |
| **Step 7** | **port** *port-num*<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# port 3799` | Configures the UDP port for CoA requests. |
| **Step 8** | **end**<br><br>**Example:**<br>`Device(config-locsvr-da-radius)# end` | Returns to privileged EXEC mode. |

# Monitoring and Troubleshooting RADIUS Change of Authorization

The following commands can be used to monitor and troubleshoot the RADIUS Change of Authorization feature:

*Table 11: Monitoring and Troubleshooting RADIUS Change of Authorization*

| Command | Purpose |
|---|---|
| **debug aaa coa** | Displays debug information for CoA processing. |
| **debug aaa pod** | Displays debug messages related to packet of disconnect (POD) packets. |
| **debug radius** | Displays information associated with RADIUS. |
| **show aaa attributes protocol radius** | Displays the mapping between an authentication, authorization, and accounting (AAA) attribute number and the corresponding AAA attribute name. |

# Configuration Examples for RADIUS Change of Authorization

## Example: Configuring RADIUS Change of Authorization

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.0.0.1
Device(config-locsvr-da-radius)# server-key cisco123
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# auth-type all
Device(config-locsvr-da-radius)# ignore session-key
Device(config-locsvr-da-radius)# ignore server-key
Device(config-locsvr-da-radius)# end
```

## Example: Configuring a Device to Ignore Bounce and Disable a RADIUS Requests

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# authentication command bounce-port ignore
Device(config)# authentication command disable-port ignore
Device(config)# end
```

# Example: Configuring the Dynamic Authorization Service for RADIUS CoA

The following example shows how to configure the device as a authentication, authorization, and accounting (AAA) server to support Change of Authorization (CoA) functionality that pushes the policy map in an input and output direction:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1
Device(config-locsvr-da-radius)# domain delimiter @
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# end
```

# Additional References for RADIUS Change of Authorization

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Security commands | • Security Command Reference: Commands A to C<br>• Security Command Reference: Commands D to L<br>• Security Command Reference: Commands M to R<br>• Security Command Reference: Commands S to Z |
| Configuring AAA | *Authentication, Authorization, and Accounting Configuration Guide* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 2903 | *Generic AAA Architecture* |

| Standard/RFC | Title |
|---|---|
| RFC 5176 | *Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)* |

### 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 |

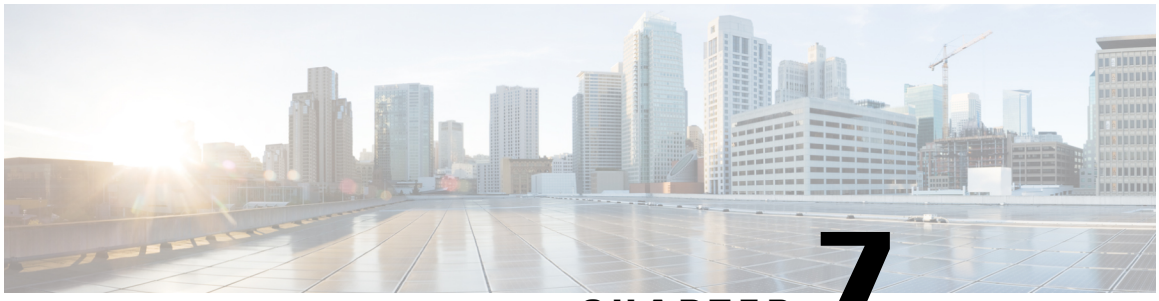
# Feature Information for RADIUS Change of Authorization

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 12: Feature Information for RADIUS Change of Authorization*

| Feature Name | Releases | Feature Information |
|---|---|---|
| RADIUS Change of Authorization | 12.2(33)SX14<br>15.1(1)SY | The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an AAA session after it is authenticated. When policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as the Cisco Secure Access Control Server (ACS), to reinitialize authentication and apply the new policy.<br>The following commands were introduced or modified: **aaa server radius dynamic-author**, **authentication command bounce-port ignore**, and **authentication command disable-port ignore**. |



CHAPTER 7

# Network Edge Authentication Topology

The Network Edge Access Topology (NEAT) feature enables extended secure access in areas outside the wiring closet (such as conference rooms). This secure access allows any type of device to authenticate on the port.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 Network Edge Authentication Topology

### IEEE 802.1X—Port-Based Network Access Control

You should understand the concepts of port-based network access control and have an understanding of how to configure port-based network access control on your Cisco platform. For more information, see the *Configuring IEEE 802.1X Port-Based Authentication* module.

The switch must be connected to a Cisco secure ACS and RADIUS authentication, authorization, and accounting (AAA) must be configured for Web authentication. If appropriate, you must enable ACL download.

If the authentication order includes the 802.1X port authentication method, you must enable IEEE 802.1X authentication on the switch.

If the authentication order includes web authentication, configure a fallback profile that enables web authentication on the switch and the interface.

**Note** The web authentication method is not supported on Cisco integrated services routers (ISRs) or Integrated Services Routers Generation 2 (ISR G2s) in Cisco IOS Release 15.2(2)T.

#### RADIUS and ACLs

You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs). For more information, see the documentation for your Cisco platform and the *Cisco IOS Security Configuration Guide: Securing User Services*.

The switch must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). For more information, see the *Configuration Guide for CISCO Secure ACS.*

# Restrictions for Network Edge Authentication Topology

- NEAT is not supported on an EtherChannel port.
- It is recommended that NEAT is only deployed with auto-configuration.
- This feature does not support standard ACLs on the switch port.

# Information About Network Edge Authentication Topology

## Authenticator and Supplicant Switch with Network Edge Authentication Topology

The NEAT feature enables extended secure access in areas outside the wiring closet (such as conference rooms). NEAT allows you to configure a switch to act as a supplicant to another switch. Thus, with NEAT enabled, the desktop switch can become a supplicant switch and authenticate itself to the access switch.

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

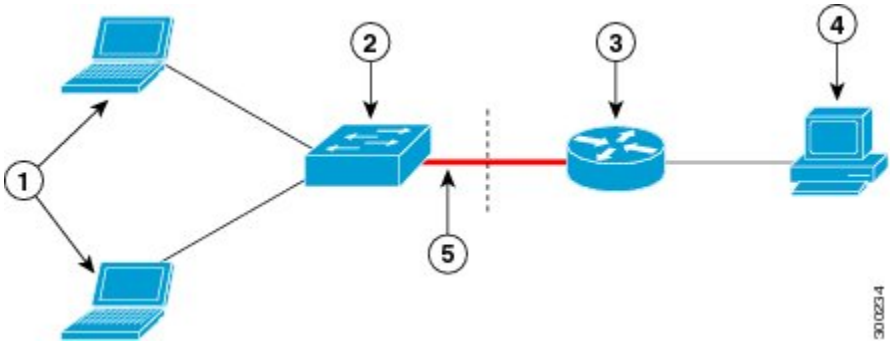
- If the access VLAN is configured on the authenticator, it becomes the native VLAN for the trunk port after successful authentication.

You can enable multidomain authentication (MDA) or multiple-authentication mode on the authenticator interface that connects to one or more supplicant switches. Multihost mode is not supported on the authenticator interface. Additional information about the authenticator can be found in the "IEEE 802.1X Authenticator" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

Use the **dot1x supplicant force-multicast** global configuration command on the supplicant switch for NEAT to work in all host modes.

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

***Figure 3: Authenticator and Supplicant Switch Using CISP***




| | | | |
|---|---|---|---|
| 1 | Workstations (clients) | 2 | Supplicant switch (outside wiring closet) |
| 3 | ISR G2 as an Authenticator | 4 | Access control server (ACS) |
| 5 | Trunk port | | |

# Guidelines for Configuring Network Edge Access Topology

- You can configure NEAT ports with the same configurations as the other authentication ports. When the supplicant switch authenticates, the port mode is changed from access-based to trunk-based on the switch vendor-specific attributes (VSAs) (device-traffic-class=switch).
- The VSA changes the authenticator switch port mode from access to trunk and enables 802.1X trunk encapsulation and the access VLAN (if any) would be converted to a native trunk VLAN. VSA does not change any of the port configurations on the supplicant.

- To change the host mode and apply a standard port configuration on the authenticator switch port, you can also use Auto Smartports user-defined macros, instead of the switch VSA. This allows you to remove unsupported configurations on the authenticator switch port and to change the port mode from access to trunk. For information, see the *AutoSmartports Configuration Guide*.

**Note** NEAT does not support redundant links between authenticator and supplicant switches.

# How to Configure Network Edge Authentication Topology

## Configuring an Authenticator with Network Edge Authentication Topology

### SUMMARY STEPS

1. **configure terminal**
2. **cisp enable**
3. **interface** *type slot/port*
4. **switchport mode access**
5. **authentication port-control auto**
6. **dot1x pae authenticator**
7. **end**
8. **show authentication interface** *interface-id*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **cisp enable**<br><br>**Example:**<br>`Switch(config)# cisp enable` | Enables CISP. |
| **Step 3** | **interface** *type slot/port*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet0/1` | Specifies the port to be configured, and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **switchport mode access**<br><br>**Example:**<br><br>`Switch(config-if)# switchport mode access` | Sets the port mode to access. |
| **Step 5** | **authentication port-control auto**<br><br>**Example:**<br><br>`Switch(config-if)# authentication port-control auto` | Sets the port-authentication mode to auto. |
| **Step 6** | **dot1x pae authenticator**<br><br>**Example:**<br><br>`Switch(config-if)# dot1x pae authenticator` | Configures the interface as a port access entity (PAE) authenticator. |
| **Step 7** | **end**<br><br>**Example:**<br><br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |
| **Step 8** | **show authentication interface** *interface-id*<br><br>**Example:**<br><br>`Switch# show authentication interface gigabitethernet0/1` | Verifies your entries. |

# Configuring a Supplicant Switch with Network Edge Authentication Topology

## SUMMARY STEPS

1. **configure terminal**
2. **cisp enable**
3. **dot1x credentials** *profile*
4. **username** *name*
5. **password** *password*
6. **exit**
7. **dot1x supplicant force-multicast**
8. **interface** *type slot/port*
9. **switchport trunk encapsulation dot1q**
10. **switchport mode trunk**
11. **dot1x pae supplicant**
12. **dot1x credentials** *profile-name*
13. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br><br>**Example:**<br>`Switch# configure terminal` | Enters global configuration mode. |
| **Step 2** | **cisp enable**<br><br>**Example:**<br>`Switch(config)# cisp enable` | Enables CISP. |
| **Step 3** | **dot1x credentials** *profile*<br><br>**Example:**<br>`Switch(config)# dot1x credentials test` | Creates a 802.1X credential profile. This must be attached to the port that is configured as supplicant. |
| **Step 4** | **username** *name*<br><br>**Example:**<br>`Switch(config-dot1x-creden)# username suppswitch` | Creates a username. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **password** *password*<br><br>**Example:**<br>`Switch(config-dot1x-creden)# password secret` | Creates a password for the new username. |
| **Step 6** | **exit**<br><br>**Example:**<br>`Switch(config-dot1x-creden)# exit` | Returns to global configuration mode. |
| **Step 7** | **dot1x supplicant force-multicast**<br><br>**Example:**<br>`Switch(config)# dot1x supplicant force-multicast` | Forces the switch to send only multicast EAPOL packets when it receives either unicast or multicast packets, which allows NEAT to work on the supplicant switch in all host modes. |
| **Step 8** | **interface** *type slot/port*<br><br>**Example:**<br>`Switch(config)# interface gigabitethernet0/1` | Specifies the port to be configured, and enters interface configuration mode. |
| **Step 9** | **switchport trunk encapsulation dot1q**<br><br>**Example:**<br>`Switch(config-if)# switchport trunk encapsulation dot1q` | Sets the port to trunk mode. |
| **Step 10** | **switchport mode trunk**<br><br>**Example:**<br>`Switch(config-if)# switchport mode trunk` | Configures the interface as a VLAN trunk port. |
| **Step 11** | **dot1x pae supplicant**<br><br>**Example:**<br>`Switch(config-if)# dot1x pae supplicant` | Configures the interface as a port access entity (PAE) supplicant. |
| **Step 12** | **dot1x credentials** *profile-name*<br><br>**Example:**<br>`Switch(config-if)# dot1x credentials test` | Attaches the 802.1X credentials profile to the interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **end**<br><br>**Example:**<br>`Switch(config-if)# end` | Returns to privileged EXEC mode. |

# Configuration Examples for Network Edge Authentication Topology

## Example: Configuring an Authenticator with NEAT

The following example shows how to configure a switch as an 802.1X authenticator:

```
Switch# configure terminal
Switch(config)# cisp enable
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport mode access
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
```

## Example: Configuring a Supplicant Switch with NEAT

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

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

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |

| 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* |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| IEEE 802.1X | *Port Based Network Access Control* |

### 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 Network Edge Authentication Topology

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 13: Feature Information for NEAT***

| Feature Name | Releases | Feature Information |
|---|---|---|
| NEAT (Network Edge Authentication Topology) | Cisco IOS 15.2(1)SY | The NEAT feature enables extended secure access in areas outside the wiring closet (such as conference rooms). This secure access allows any type of device to authenticate on the port. |