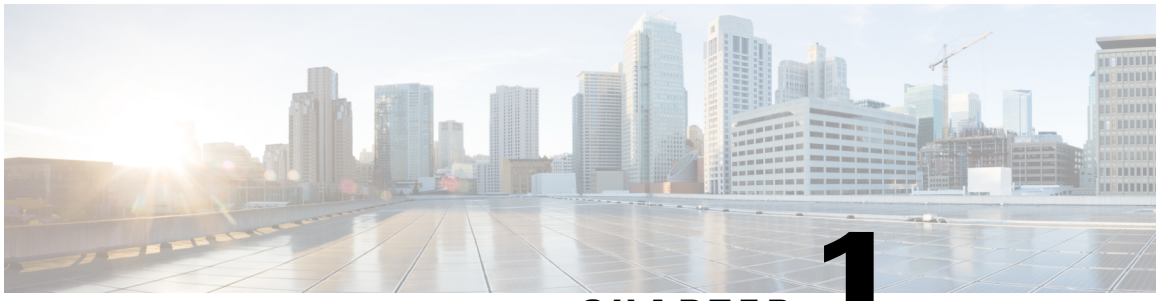
802.1X Authentication Services Configuration Guide, Cisco IOS Release 15S

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 at the end of this module.

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.

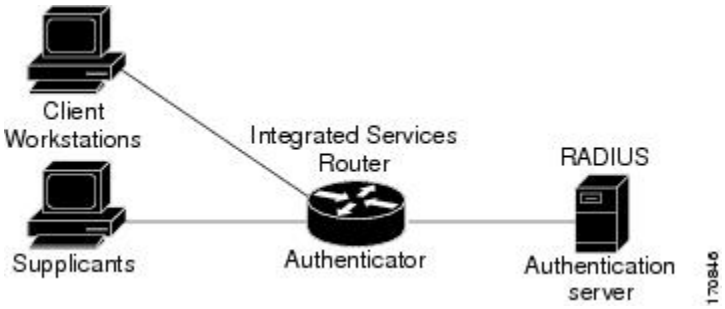
Note To ensure that information about any IEEE 802.1x-related commands that is entered on a port is automaticallly added to the running configuration to address any backward compatibility issues, use the **dot1x pae authenticator** command.

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.

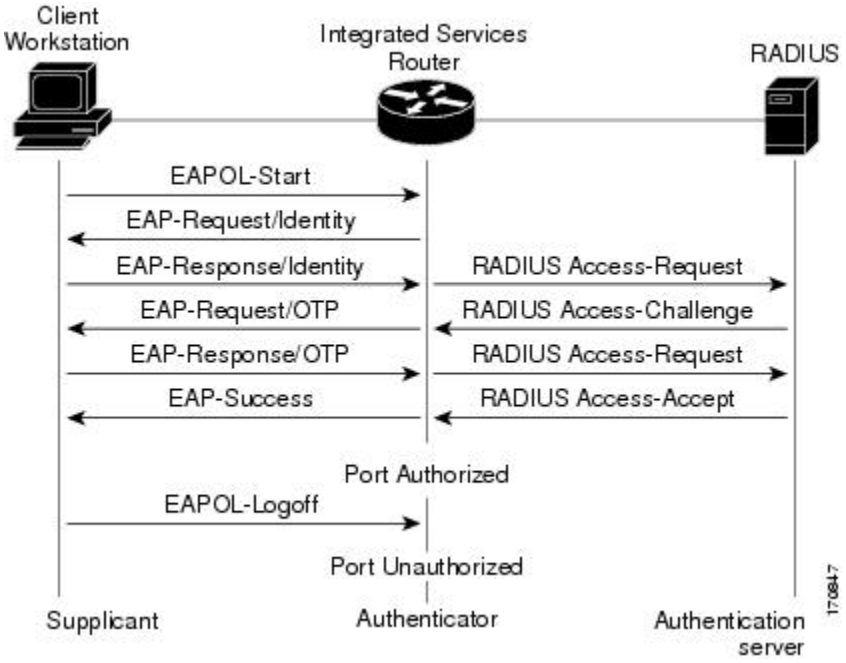
However, if during bootup the supplicant does not receive an EAP-request/identity frame from the router, the supplicant can initiate authentication by sending an EAPOL-start frame, which prompts the router to request the supplicant's identity.

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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication dot1x** {**default** | *listname*} *method1* [*method2...*] **Example:** `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** **Example:** `Device(config)# dot1x system-auth-control`	Globally enables 802.1X port-based authentication.
Step 6	**identity profile default** **Example:** `Device(config)# identity profile default`	Creates an identity profile and enters dot1x profile configuration mode.
Step 7	**interface** *type slot/port* **Example:** `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**} **Example:** `Device(config-if)# authentication port-control auto`	Enables 802.1X port-based authentication on the interface. • **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. • **force-authorized-—**Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting. • **force-unauthorized—**Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. The router cannot provide authentication services to the supplicant through the port. **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**] **Example:** `Device(config-if)# dot1x pae authenticator`	Sets the Port Access Entity (PAE) type. • **supplicant—**The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator. • **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** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 11	**show dot1x** **Example:** `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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius-server vsa send authentication** **Example:** `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* **Example:** `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**] **Example:** `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. • The **multi-auth** keyword specifies multiple authentications to occur on the 802.1X-authorized port. • 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. • The **multi-host** keyword specifies multiple hosts on the 802.1X-authorized port. • The **single-host** keyword specifies a single client on the 802.1X-authorized port. • (Optional) The **open** keyword specifies that the port is open; that is, there are no access restrictions.
Step 6	**switchport voice vlan** *vlan-id* **Example:** `Device(config-if)# switchport voice vlan 2`	(Optional) Configures the voice VLAN.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 8	**show authentication interface** *type number* **Example:** `Device# show authentication interface`	Displays your entries.

	Command or Action	Purpose
Step 9	**copy running-config startup-config** **Example:** `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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps dot1x** *notification-type* **Example:** `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 • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • 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 • 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: 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

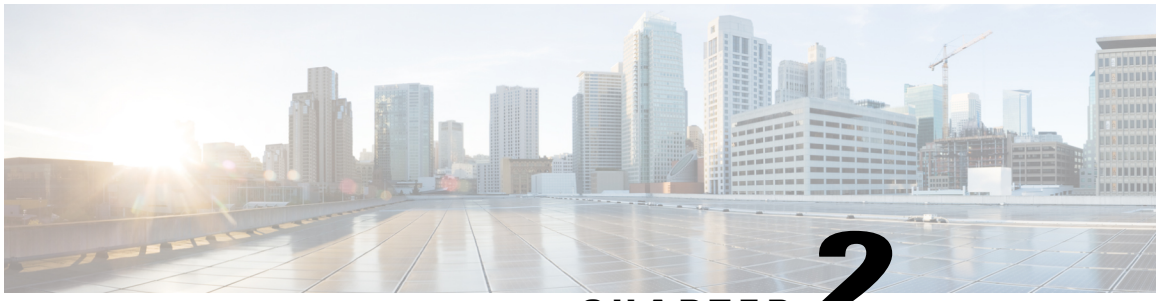
Feature Name	Releases	Feature Information
CDP Enhancement —Host Presence TLV	Cisco IOS 15.2(2)T Cisco IOS 15.2(1)E	This features allows you to ensure that only one client can be connected to the 802.1X-enabled port. The switch detects the client by sending an EAPOL frame when the port link state changes 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. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E

Feature Name	Releases	Feature Information
IEEE 802.1X Authenticator	Cisco IOS 12.3(4)T Cisco IOS 15.2(2)T Cisco IOS 15.3(1)S Cisco IOS 15.2(1)E	This feature was introduced to prevent unauthorized devices (supplicants) from gaining access to the network. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E 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	Cisco IOS 15.2(2)T Cisco IOS 15.2(1)E	The IEEE 802.1X-Conditional Logging feature is used for troubleshooting interfaces. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E

Feature Name	Releases	Feature Information
IEEE 802.1X MIB Support	Cisco IOS 12.4(11)T Cisco IOS 15.2(1)E	This feature provides support for the following MIBs: • Cisco-PAE-MIB • IEEE8021-PAE-MIB In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 89x Series ISR • Cisco 88x Series ISR In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E

Feature Name	Releases	Feature Information
IEEE 802.1X Support for Trunk Ports	Cisco IOS 15.2(1)E	The IEEE 802.1X Support for Trunk Ports feature is used to configure Ethernet interfaces as trunk ports. In Cisco IOS XE 15.2(1)E, this feature was supported on the following platforms: • Catalyst 2960-C Series Switches • Catalyst 2960-S Series Switches • Catalyst 3560-C Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches • Catalyst 4500E Supervisor Engine 6-E • Catalyst 4500E Supervisor Engine 6L-E



CHAPTER 2

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 at the end of this module.

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 2: Accounting AV Pairs

Attribute Number	AV Pair Name	*START*	*INTERIM*	*STOP*
Attribute [1]	User-Name	Always	Always	Always
Attribute [4]	NAS-IP-Address	Always	Always	Always
Attribute [5]	NAS-Port	Always	Always	Always
Attribute [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 3: 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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA globally.
Step 4	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **acct-port** *port-number* **Example:** | `Device(config)# radius-server host 172.20.39.46 auth-port 1812 acct-port 1813 key rad123`	Specifies a RADIUS server host. • The **auth-port** keyword and *port-number* argument specifies the User Datagram Protocol (UDP) destination port for authentication requests. • 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** **Example:** `Device(config)# aaa accounting dot1x default start-stop group radius`	Provides information about all IEEE 802.1x-related user events. • 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. • 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** **Example:** `Device(config)# aaa accounting system default start-stop group radius`	Performs accounting for all system-level events not associated with users, such as reloads. **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. • 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. • 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** **Example:** `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 • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • 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 • 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: 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

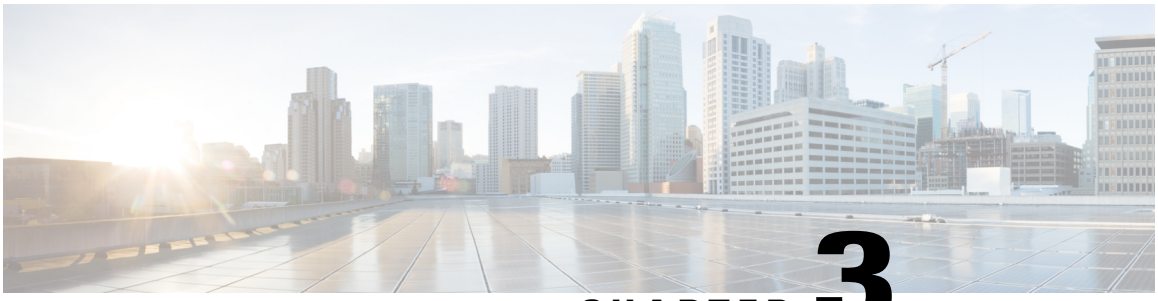
Feature Information for IEEE 802.1X RADIUS Accounting

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 4: Feature Information for IEEE 802.1X RADIUS Accounting

Feature Name	Releases	Feature Information
IEEE 802.1X RADIUS Accounting	Cisco IOS 12.4(11)T Cisco IOS 15.3(1)S	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. In Cisco IOS Release 12.4(11)T, this feature was introduced on the following Cisco ISRs equipped with cards or modules that include switch ports: • Cisco 89x Series ISR • Cisco 88x Series ISR



CHAPTER 3

IEEE 802.1X Flexible Authentication

The IEEE 802.1X Flexible Authentication feature provides a means of assigning authentication methods to ports and specifying the order in which the methods are executed when an authentication attempt fails. Using this feature, you can control which ports use which authentication methods, and you can control the failover sequencing of methods on those 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 at the end of this module.

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 Flexible Authentication

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.

Before you can use the IEEE 802.1X Flexible Authentication feature, the switch must be connected to a Cisco secure access control server (ACS) and RADIUS authentication, authorization, and accounting (AAA) must be configured for web authentication. If appropriate, you must enable access control list (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.

RADIUS and ACLs

You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply 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 ACS. For more information, see the Configuration Guide for *Cisco Secure ACS*.

Restrictions for IEEE 802.1X Flexible Authentication

- The web authentication method cannot fail over to the 802.1X or the MAC Authentication Bypass (MAB) authentication method.

Note No authentication method can follow web authentication in the configuration order. Web authentication must be the last method configured.

- 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.
- Layer 2 web authentication is not supported with flexible authentication.
- This feature does not support standard ACLs on the switch 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) will fail 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* will fail if the access VLAN and voice VLAN have been configured with the same VLAN ID.

Information About IEEE 802.1X Flexible Authentication

Overview of the Cisco IOS Auth Manager

The capabilities of devices connecting to a given network can be different, thus requiring that the network support different authentication methods and authorization policies. The Cisco IOS Auth Manager handles network authentication requests and enforces authorization policies, regardless of authentication method. The Auth Manager maintains operational data for all port-based network connection attempts, authentications, authorizations, and disconnections and, as such, serves as a session manager.

The possible states for Auth Manager sessions are:

- Authc Success—The authentication method has run successfully. This is an intermediate state.
- Authc Failed—The authentication method has failed. This is an intermediate state.
- Authz Success—All features have been successfully applied for this session. This is a terminal state.
- Authz Failed—At least one feature has failed to be applied for this session. This is a terminal state.
- Idle—In the idle state, the authentication session has been initialized, but no methods have yet been run. This is an intermediate state.
- No methods—No method provided a result for this session. This is a terminal state.
- Running—A method is currently running. This is an intermediate state.

IEEE 802.1X Flexible Authentication Methods

The IEEE 802.1X Flexible Authentication feature supports three authentication methods:

- dot1X—IEEE 802.1X authentication is a Layer 2 authentication method.
- mab—MAC-Authentication Bypass is a Layer 2 authentication method.
- webauth—Web authentication is a Layer 3 authentication method.

IEEE 802.1X Host Mode Authentication

The IEEE 802.1X Flexible Authentication feature supports the following host modes:

- multi-auth—Multiauthentication allows one authentication on a voice VLAN and multiple authentications on the data VLAN.
- multi-domain—Multidomain authentication allows two authentications: one on the voice VLAN and one on the data VLAN.

IEEE 802.1X Authentication Order and Authentication Priority

The IEEE 802.1X Flexible Authentication feature enables authentication order and authentication priority. The **authentication order** command sets the default authentication priority. You can use the **authentication priority** command to override the default authentication priority. For example, you might specify an authentication order of MAB and 802.1X. However, after authorization, you might not want to ignore subsequent 802.1X handshakes. In this case, you can give the 802.1X authentication method a higher priority than the MAB method.

How to Configure IEEE 802.1X Flexible Authentication

Configuring Authentication Order

Authentication order is configured on individual ports to control which ports use which authentication methods.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot1x system-auth-control**
4. **interface type** *slot/port*
5. **switchport**
6. **switchport mode access**
7. **switchport access vlan** *vlan-id*
8. **mab** [**eap**]
9. **authentication port-control**{**auto**|**force-authorized**|**force unauthorized**}
10. **authentication** *fallback profile*
11. **authentication order**{**dot1x** [**mab** |**webauth**][**webauth**] |**mab** [**dot1x**|**webauth**] [**webauth**] |**webauth**}
12. **dot1x pae authenticator**
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot1x system-auth-control** **Example:** `Router(config)# dot1x system-auth-control`	(Optional) Enables IEEE 802.1x authentication globally on the switch. • Enable IEEE 802.1x authentication if the authentication order includes the **dot1x** authentication method.
Step 4	**interface type** *slot/port* **Example:** `Router(config)# interface FastEthernet 2/1`	Enters interface configuration mode.
Step 5	**switchport** **Example:** `Router(config-if)# switchport`	Places the interface in Layer 2-switched mode.
Step 6	**switchport mode access** **Example:** `Router(config-if)# switchport mode access`	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
Step 7	**switchport access vlan** *vlan-id* **Example:** `Router(config-if)# switchport access vlan 2`	Sets the VLAN for the port.
Step 8	**mab** [**eap**] **Example:** `Router(config-if)# mab`	(Optional) Enables MAB. • Enable MAB if the authentication order includes the **mab** keyword (see Step 11).
Step 9	**authentication port-control**{**auto**|**force-authorized**|**force unauthorized**} **Example:** `Router(config-if)# authentication port-control auto`	Configures the authorization state of the port.
Step 10	**authentication** *fallback profile* **Example:** `Router(config-if)# authentication fallback web-profile`	Configures the authorization state of the port and enables web authentication. • Enable web authentication if the authentication order includes the **webauth** keyword (see Step 11).

	Command or Action	Purpose
Step 11	**authentication order** {**dot1x** [**mab** |**webauth**][**webauth**] |**mab** [**dot1x**|**webauth**] [**webauth**] |**webauth**} **Example:** `Router(config-if)# authentication order mab dot1x webauth`	Configures the authentication order.
Step 12	**dot1x pae authenticator** **Example:** `Router(config-if)# dot1x pae authenticator`	Enables the port to respond to messages meant for an IEEE 802.1x authenticator.
Step 13	**end** **Example:** `Router(config-if)# end`	Returns to global configuration mode.

Configuring Authentication Priority

Authentication priority is configured to control the fail-over sequencing of methods on individual ports.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *typeslot/port*
4. **authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *typeslot/port* **Example:** `Switch(config)# interface FastEthernet 2/1`	Enters interface configuration mode.
Step 4	**authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**} **Example:** `Switch(config-if)# authentication priority dot1x mab webauth`	Configures authentication priority.
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to global configuration mode.

Configuration Examples for IEEE 802.1X Flexible Authentication

Example: Configuring IEEE 802.1X Flexible Authentication

The following example shows the commands used to configure the port in multiple authentication host mode. The order of authentication is 802.1X first, then MAB, and finally web authentication:

```
enable
configure terminal
dot1x system-auth-control

aaa new-model
aaa authentication login default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa session-id common
ip http server

ip admission name webauth-rule proxy http
fallback profile webauth-profile
 ip access-group webauthlist in
 ip admission webauth-rule

interface GigabitEthernet 2/1
 switchport
 switchport mode access
 switchport access vlan 125
 switchport voice vlan 127
 mab
 authentication port-control auto
 authentication fallback webauth-profile
 authentication host-mode multi-auth
 authentication order dot1x mab webauth
 dot1x pae authenticator
```

Additional References

Related Documents

Related Topic	Document Title
Authentication commands	*Cisco IOS Security Command Reference Commands A to C*
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* • *Catalyst 3750 Switch Command Reference, Cisco IOS Release 12.2(25)SEE*
IPSec	• *IPsec Management Configuration Guide, Cisco IOS Release 15.2MT* • *Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15.2MT* • *Security for VPNs with IPsec Configuration Guide, Cisco IOS Release 15.2MT*
RADIUS	*RADIUS Configuration Guide, Cisco IOS Release 15.2MT*
Standalone MAB support	*Standalone MAB Support*
Port-based network access control	"Configuring IEEE 802.1X Port-Based Authentication"*Configuring IEEE 802.1X Port-Based Authentication* module. module.

Standards and RFCs

Standard/RFC	Title
IEEE 802.1X protocol	—
RFC 3580	IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)

MIBs

MIB	MIBs Link
• CISCO–AUTH–FRAMEWORK–MIB • CISCO–MAC–AUTH–BYPASS–MIB • CISCO–PAE–MIB • 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: 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 Flexible 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 5: Feature Information for IEEE 802.1X Flexible Authentication

Feature Name	Releases	Feature Information
IEEE 8021.X Flexible Authentication	Cisco IOS 12.2(33)SXI Cisco IOS 15.2(2)T	This feature provides a means of configuring ports with one or more authentication methods and specifying the order in which those authentication methods are attempted. The following commands were introduced or modified: **authentication fallback**, **authentication hostmode**, **authentication order**, **authentication port-control** **authentication priority**, **authentication timer restart**, **debug authentication**, **mab**, **show authentication interface**, **show authentication registrations**, **show authentication sessions**, **showmab**. The following commands were removed or made obsolete: **dot1x fallback**, **dot1x host-mode**, **dot1x port-control**.