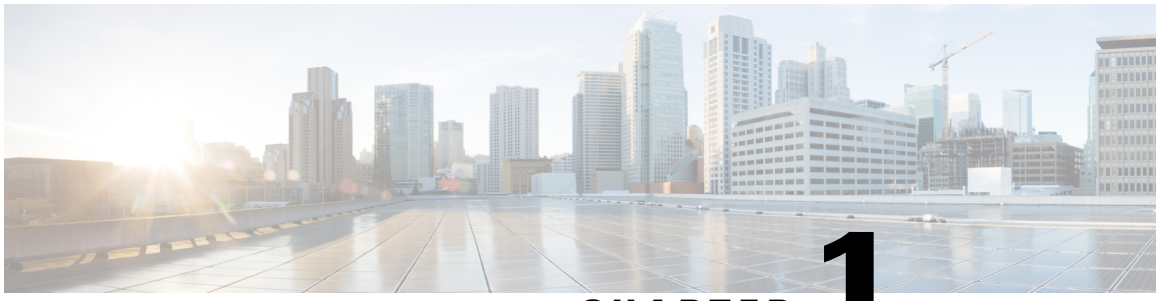
802.1X Authentication Services Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)

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.
- By default, authentication system messages, MAC authentication by-pass system messages and 802.1x system messages are not displayed. If you need to see these system messages, turn on the logging manually, using the following commands:
  - **authentication logging verbose**
  - **dot1x logging verbose**
  - **mab logging verbose**

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.

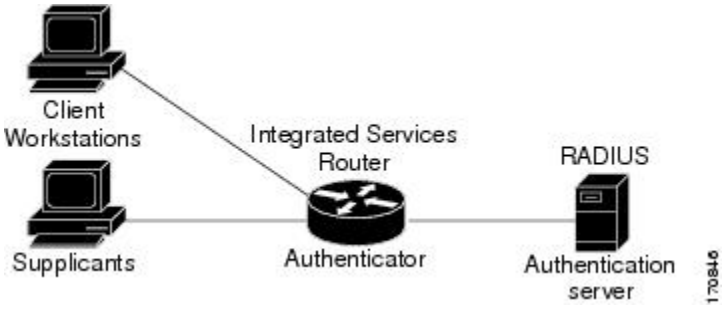
Note To ensure that information about any IEEE 802.1x-related commands that is entered on a port is automaticallly added to the running configuration to address any backward compatibility issues, use the **dot1x pae authenticator** command.

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.

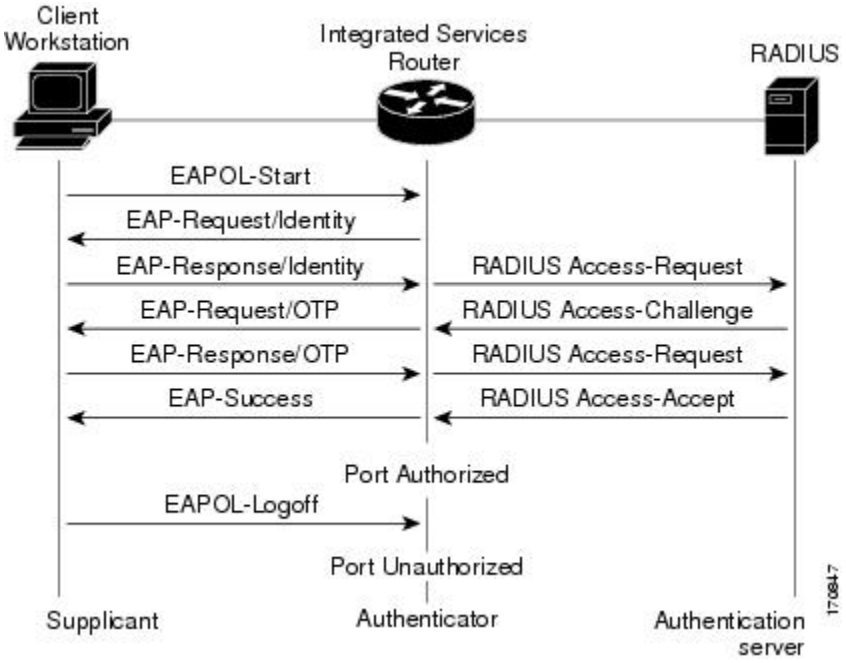
However, if during bootup the supplicant does not receive an EAP-request/identity frame from the router, the supplicant can initiate authentication by sending an EAPOL-start frame, which prompts the router to request the supplicant's identity.

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. **access-session 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 Gigabitethernet 1/0/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 8	**access-session port-control** {**auto** | **force-authorized** | **force-unauthorized**} **Example:** `Device(config-if)# access-session 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 Device 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 Device 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 Device 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. **access-session 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 Gigabitethernet 1/2/1`	Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode.
Step 5	**access-session host-mode** {**multi-auth** | **multi-domain** | **multi-host** | **single-host**} [**open**] **Example:** `Device(config-if)# access-session host-mode single-host Gigabitethernet 1/2/1`	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:** `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	**snmp-server enable traps dot1x** *notification-type* **Example:** `Device(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
Device-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 XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.5E Cisco IOS XE Release 3.6E	

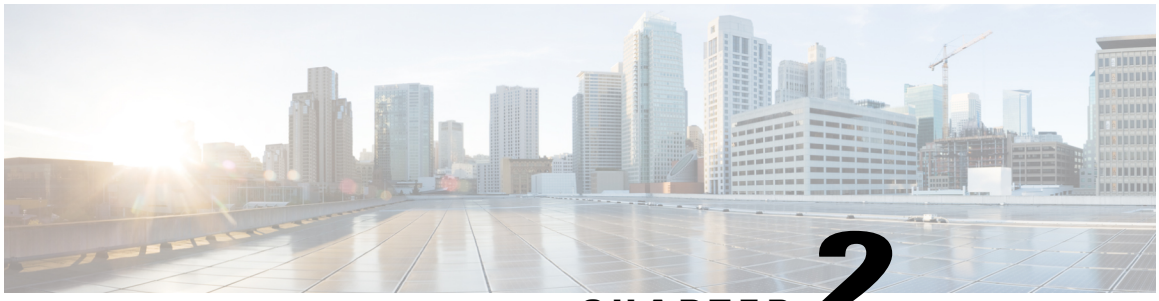
Feature Name	Releases	Feature Information
		This features allows you to ensure that only one client can be connected to the 802.1X-enabled port. The switch detects the client by sending an EAPOL frame when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.5E, this feature was supported on the following platforms: • Catalyst 4900 Series Switches • Catalyst 4500E Supervisor Engine 7-E • Catalyst 4500E Supervisor Engine 7L-E In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.

Feature Name	Releases	Feature Information
IEEE 802.1X Authenticator	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.5E Cisco IOS XE Release 3.6E	This feature was introduced to prevent unauthorized devices (supplicants) from gaining access to the network. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.5E, this feature was supported on the following platforms: • Catalyst 4900 Series Switches • Catalyst 4500E Supervisor Engine 7-E • Catalyst 4500E Supervisor Engine 7L-E In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers. 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 XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.5E Cisco IOS XE Release 3.6E	The IEEE 802.1X-Conditional Logging feature is used for troubleshooting interfaces. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.5E, this feature was supported on the following platforms: • Catalyst 4900 Series Switches • Catalyst 4500E Supervisor Engine 7-E • Catalyst 4500E Supervisor Engine 7L-E Cisco IOS XE Release 3.6E In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.

Feature Name	Releases	Feature Information
IEEE 802.1X MIB Support	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.5E Cisco IOS XE Release 3.6E	This feature provides support for the following MIBs: • Cisco-PAE-MIB • IEEE8021-PAE-MIB In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.5E, this feature was supported on the following platforms: • Catalyst 4900 Series Switches • Catalyst 4500E Supervisor Engine 7-E • Catalyst 4500E Supervisor Engine 7L-E In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.

Feature Name	Releases	Feature Information
IEEE 802.1X Support for Trunk Ports	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE 3.5E Cisco IOS XE Release 3.6E	The IEEE 802.1X Support for Trunk Ports feature is used to configure Ethernet interfaces as trunk ports. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.5E, this feature was supported on the following platforms: • Catalyst 4900 Series Switches • Catalyst 4500E Supervisor Engine 7-E • Catalyst 4500E Supervisor Engine 7L-E In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



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 • 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

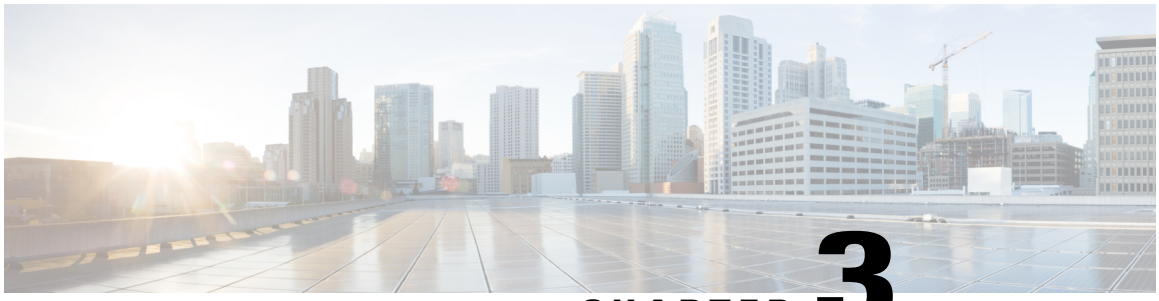
Feature Information for IEEE 802.1X Common Session ID

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	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	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. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



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** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode. • 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** **Example:** `Switch(config-if)# authentication port-control auto`	Enables 802.1X authentication on the port.
Step 4	**exit** **Example:** `Switch(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 5	**dot1x guest-vlan supplicant** **Example:** `Switch(config)# dot1x guest-vlan supplicant`	Specifies the supplicant as an 802.1X guest VLAN. • You can configure any active VLAN except an RSPAN VLAN or a voice VLAN as an 802.1X guest VLAN.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show authentication interface** *interface-id* **Example:** `Switch# show authentication interface gigabitethernet0/1`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `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 • 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

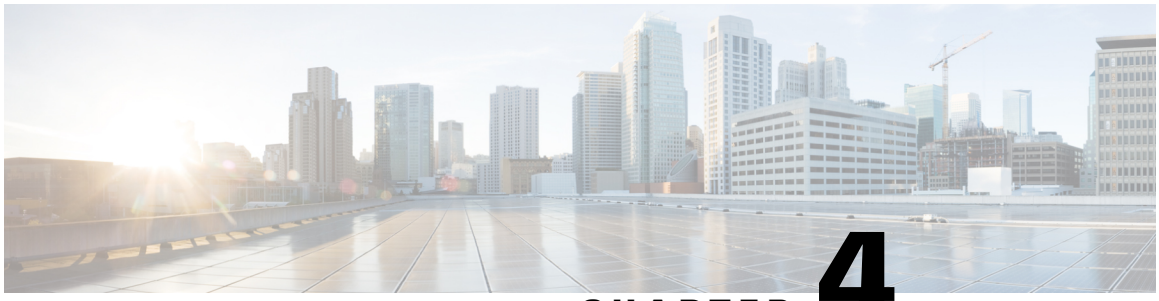
Feature Information for IEEE 802.1X Guest VLAN

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	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	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. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



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** **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.

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius-server host 172.20.39.46 auth-port 1812 acct-port 1813 key rad123
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# aaa accounting system default start-stop group radius
Device(config)# end
Device#
```

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

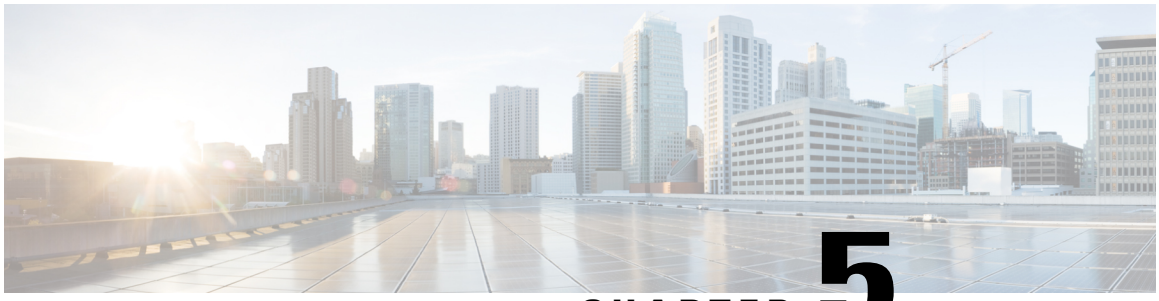
Feature Information for IEEE 802.1X RADIUS Accounting

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 6: Feature Information for IEEE 802.1X RADIUS Accounting

Feature Name	Releases	Feature Information
IEEE 802.1X RADIUS Accounting	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	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 XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 5

IEEE 802.1X Voice VLAN

The IEEE 802.1X Voice VLAN feature allows you to configure a special access port associated with two VLAN identifiers. One identifier carries voice traffic to and from the IP phone. The other identifier carries data traffic to and from the workstation connected to the router through the IP phone.

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 Voice VLAN

The following tasks must be completed before implementing the IEEE 802.1X Voice 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 Voice VLAN 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 Voice VLAN

- The IEEE 802.1X Authentication with Voice VLAN feature is available only on a switch port.
- This feature does not support standard ACLs on the switch port.
- If the VLAN to which an IEEE 802.1X port is assigned is shut down, disabled, or removed, then 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.
- If you try to change the mode (for example, from access to trunk) of an IEEE 802.1X-enabled port, an error message appears, and the port mode is not changed.
- 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 the same VLAN ID for both access and voice traffic.
- When access and voice VLAN are configured to the same ID, you cannot configure IEEE 802.1X authentication on the port.
- The IEEE 802.1X protocol is supported on Layer 2 static-access ports, voice VLAN-enabled ports, and Layer 3 routed ports, but it is not supported on 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.
    - Trunk port—If you try to enable IEEE 802.1X authentication on a trunk port, an error message appears, and IEEE 802.1X authentication is not enabled. If you try to change the mode of an IEEE 802.1X-enabled port to trunk, an error message appears, and the port mode is not changed.

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

Information About IEEE 802.1X Voice VLAN

IEEE 802.1X Authentication with Voice VLAN

The IEEE 802.1X Authentication with Voice VLAN feature is available only on a switch port.

A voice VLAN port is a special access port associated with two VLAN identifiers:

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

The IP phone uses the VVID for its voice traffic, regardless of the authorization state of the port. This allows the phone to work independently of IEEE 802.1X authentication.

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

A voice VLAN port becomes active when there is a link, and the device MAC address appears after the first Cisco Discovery Protocol message from the IP phone. Cisco IP phones do not relay Cisco Discovery Protocol messages from other devices. As a result, if several IP phones are connected in series, the router recognizes only the one directly connected to it. When IEEE 802.1X authentication is enabled on a voice VLAN port, the router drops packets from unrecognized IP phones more than one hop away.

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

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

IEEE 802.1X Voice VLAN Configuration

A port connected to the Cisco IP Phone can be configured to send CDP packets to the phone that configures the way in which the phone sends voice traffic. The phone can carry voice traffic in IEEE 802.1Q frames for a specified voice VLAN with a Layer 2 CoS value. It can use IEEE 802.1p priority tagging to give voice traffic a higher priority and forward all voice traffic through the native (access) VLAN. The Cisco IP Phone can also send untagged voice traffic or use its own configuration to send voice traffic in the access VLAN. In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5).

Note See your Cisco switch software configuration guide for additional Voice VLAN information.

How to Configure IEEE 802.1X Voice VLAN

Configuring an IEEE 802.1X Voice VLAN

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mls qos**
4. **interface** *interface-id*
5. **mls qos trust cos**
6. **switchport voice** {**detect cisco-phone** [**full-duplex**] | **vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}}
7. **end**
8. **show interfaces** *interface-id* **switchport**

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	**mls qos** **Example:** `Device(config)# mls qos`	Enables quality of service (QoS) functionality globally.
Step 4	**interface** *interface-id* **Example:** `Device(config)# interface Gigabitethernet 1/0/1`	Specify the interface connected to the phone, and enter interface configuration mode.
Step 5	**mls qos trust cos** **Example:** `Device(config-if)# mls qos trust cos`	Configure the interface to classify incoming traffic packets by using the packet CoS value. For untagged packets, the port default CoS value is used.

	Command or Action	Purpose
Step 6	**switchport voice** {**detect cisco-phone** [**full-duplex**] | **vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}} **Example:** `Device(config-if)# switchport voice vlan dot1p`	Configures how the Cisco IP Phone carries voice traffic: • **detect—**Configure the interface to detect and recognize a Cisco IP phone. • **cisco-phone—**When you initially implement the switchport voice detect command, this is the only allowed option. The default is **no switchport voice detect cisco-phone**. • **full-duplex—**(Optional) Configure the switch to only accept a full-duplex Cisco IP phone. • *vlan-id***—**Configure the phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP Phone forwards the voice traffic with an IEEE 802.1Q priority of 5. Valid VLAN IDs are 1 to 4094. • **dot1p—**Configure the phone to use IEEE 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. By default, the Cisco IP Phone forwards the voice traffic with an IEEE 802.1p priority of 5. • **none—**Allow the phone to use its own configuration to send untagged voice traffic. • **untagged—**Configure the phone to send untagged voice traffic.
Step 7	**end** **Example:** `Device(config-if)# end`	Return to privileged EXEC mode.
Step 8	**show interfaces** *interface-id* **switchport** **Example:** `Device# show interfaces Gigabitethernet 1/0/1 switchport`	Verify your QoS and voice VLAN entries.

What to Do Next

Note See your Cisco switch software configuration guide for additional Voice VLAN configuration information.

Configuration Example for IEEE 802.1X Voice VLAN

Example: IEEE 802.1X Voice VLAN Configuration

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

```
Device# configure terminal
Device(config)# interface Gigabitethernet 1/5/9
Device(config-if)# switchport access vlan 2
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan 10
Device(config-if)# dot1x pae authenticator
Device(config-if)# dot1x port-control auto
Device(config-if)# end
Device(config# end
Device#
```

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

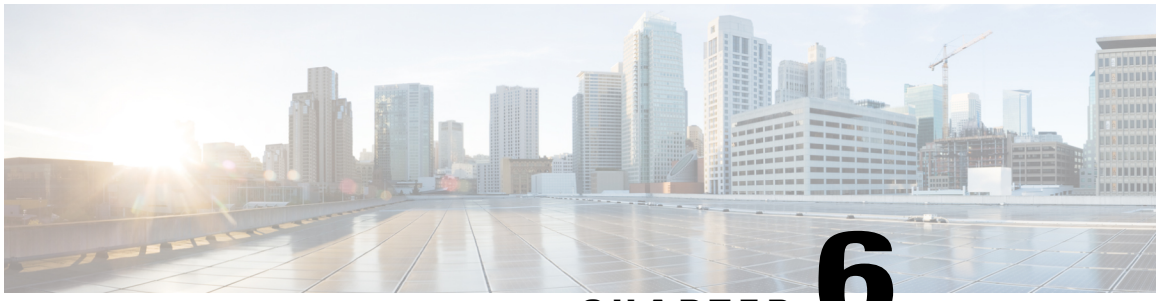
Feature Information for IEEE 802.1X Voice VLAN

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 7: Feature Information for IEEE 802.1X Voice VLAN

Feature Name	Releases	Feature Information
IEEE 802.1X Voice VLAN	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	The IEEE 802.1X Voice VLAN feature allows you to configure a special access port associated with two VLAN identifiers. One identifier carries voice traffic to and from the IP phone. The other identifier carries data traffic to and from the workstation connected to the router through the IP phone. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 6

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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authorization network radius if-authenticated** **Example:** `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** **Example:** `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** **Example:** `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. **access-session 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.
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 Gigabitethernet 1/0/1`	Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.
Step 8	**access-session port-control** {**auto** | **force-authorized** | **force-unauthorized**} **Example:** `Device(config-if)# access-session 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 Device 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 Device 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 Device 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. • **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.

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 • 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

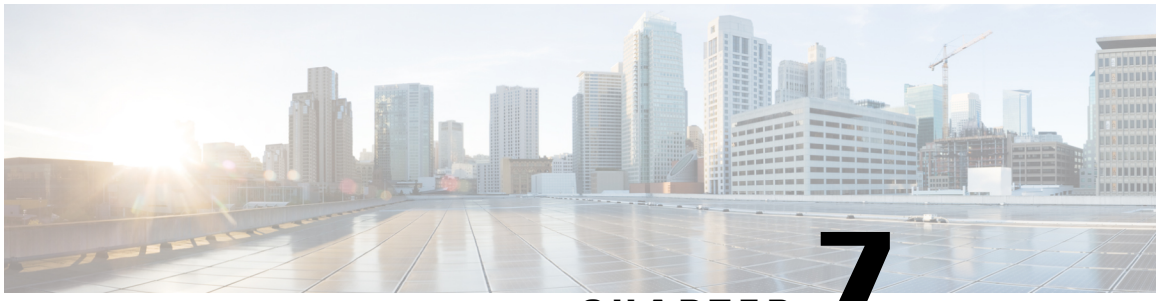
Feature Information for IEEE 802.1X VLAN Assignment

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 8: Feature Information for IEEE 802.1X VLAN Assignment

Feature Name	Releases	Feature Information
IEEE Information for IEEE 802.1X VLAN Assignment	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	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. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 7

IEEE 802.1X Multiple Authentication

The IEEE 802.1X Multiple Authentication feature provides a means of authenticating multiple hosts on a single port. With both 802.1X and non-802.1X devices, multiple hosts can be authenticated using different methods. Each host is individually authenticated before it can gain access to the network resources.

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 Multiple 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.

Before you can use the IEEE 802.1X Multiple Authentication feature, the switch must be connected to a Cisco secure Access Control Server and RADIUS authentication, authorization, and accounting (AAA) must be configured for web authentication. ACL download must be enabled.

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 access control lists (ACLs).

The switch must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS).

Restrictions for IEEE 802.1X Multiple Authentication

- Only one voice VLAN is supported on a multiple authentication port.
- You cannot configure a guest VLAN or an authentication failed VLAN in multiple authentication mode.
- When a port is in multiple authentication mode, the guest VLAN and authentication failed VLAN features do not activate.
- In multiple authentication mode, only multicast EAPOL packets are accepted by the port.
- The web authentication method is not supported on Cisco integrated services routers (ISRs) or Integrated Services Routers Generation 2 (ISR-G2s) in Cisco IOS 15.2(2)T.
- Inactivity aging is not supported on Cisco ISRs or ISR-G2s in multiple authentication mode.
- 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 Multiple Authentication

Guidelines for Configuring IEEE 802.1X Multiple Authentication

Assign a RADIUS-server-supplied VLAN in multiple authentication mode, under these conditions:

- The host is the first host authorized on the port, and the RADIUS server supplies VLAN information.
- Subsequent hosts are authorized with a VLAN that matches the operational VLAN.

- A host is authorized on the port with no VLAN assignment, and subsequent hosts either have no VLAN assignment, or their VLAN information matches the operational VLAN.
- The first host authorized on the port has a group VLAN assignment, and subsequent hosts either have no VLAN assignment, or their group VLAN matches the group VLAN on the port. Subsequent hosts must use the same VLAN from the VLAN group as the first host. If a VLAN list is used, all hosts are subject to the conditions specified in the VLAN list.
- Only one voice VLAN assignment is supported on a multi-auth port .
- After a VLAN is assigned to a host on the port, subsequent hosts must have matching VLAN information or be denied access to the port.
- You cannot configure a guest VLAN or an auth-fail VLAN in multi-auth mode.
- The behavior of the critical-auth VLAN is not changed for multi-auth mode. When a host tries to authenticate and the server is not reachable, all authorized hosts are reinitialized in the configured VLAN.

How to Configure IEEE 802.1X Multiple Authentication

Configuring IEEE 802.1X Multiple Authentication

Beginning in privileged EXEC mode, follow these steps to allow one client on the voice VLAN and multiple authenticated clients on the data VLAN, where each host is individually authenticated.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius-server vsa send authentication**
4. **interface** *interface-id*
5. **access-session host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] *interface-id*
6. **end**
7. **show access-session interface** *interface-id*
8. **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** *interface-id* **Example:** `Device(config)# interface Gigabitethernet 1/2/1`	Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode.
Step 5	**access-session host-mode** [**multi-auth** | **multi-domain** | **multi-host** | **single-host**] *interface-id* **Example:** `Device(config-if)# access-session host-mode multi-auth`	Allows one client on the voice VLAN and multiple authenticated clients on the data VLAN. • Each host is individually authenticated.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show access-session interface** *interface-id* **Example:** `Device# show access-session interface g1/0/23`	Verifies the entries.
Step 8	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves entries in the configuration file.

Configuration Examples for IEEE 802.1X Multiple Authentication

Example: Configuring IEEE 802.1X Multiple Authentication

```
aaa new-model
!
!
aaa authentication login CON local
```

```
aaa authentication login VTY local
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting auth-proxy default start-stop group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
!
aaa session-id common
!
dot1x system-auth-control
!

interface Gigabitethernet1/1/1
 switchport access vlan 20
 switchport voice vlan 117
 no ip address
 authentication host-mode multi-auth
 authentication order mab
 authentication port-control auto
 mab
 dot1x pae authenticator
end
```

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 Command Reference, Cisco IOS 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

Standards

Standard	Title
IEEE 802.1X protocol	—

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

RFCs

RFC	Title
RFC-3580	IEEE 802.1x 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

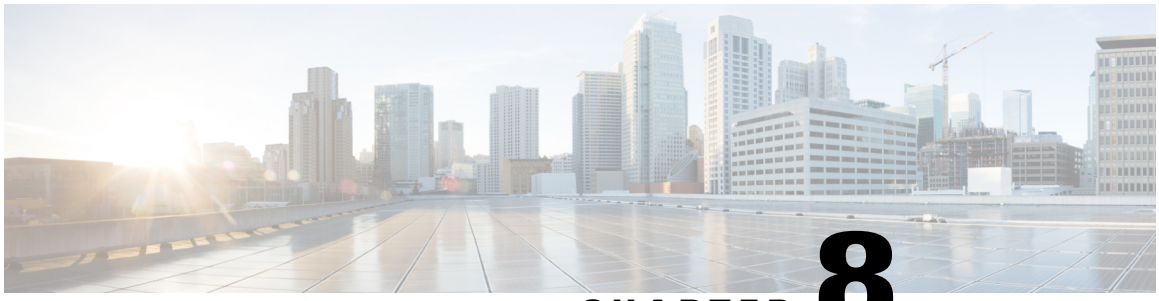
Feature Information for IEEE 802.1X Multiple Authentication

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 9: Feature Information for IEEE 802.1X Multiple Authentication

Feature Name	Releases	Feature Information
IEEE 8021.X Multiple Authentication	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	The IEEE 802.1X Multiple Authentication feature provides a means of authenticating multiple hosts on a single port. With both 802.1X and non-802.1X devices, multiple hosts can be authenticated using different methods. Each host is individually authenticated before it can gain access to the network resources. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. The following commands were introduced or modified: **authentication host-mode**. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 8

IEEE 802.1X Multidomain Authentication

Multidomain authentication (MDA) allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch 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 IEEE 802.1X Multidomain 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.

The switch must be connected to a Cisco secure Access Control System (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 IEEE 802.1X Multidomain Authentication

- In multidomain authentication mode, only multicast EAPOL packets are accepted by the port.
- Inactivity aging is not supported on Cisco integrated services routers (ISRs) or Integrated Services Routers Generation 2 (ISR-G2s) in multidomain authentication mode.
- In multidomain authentication mode, the CDP 2nd port disconnect feature is supported.
- 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 Multidomain Authentication

Guidelines for Configuring IEEE 802.1X Multidomain Authentication

MDA allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port. The port is divided into a data domain and a voice domain.

Note When an access port is configured for multidomain authentication, the LED of a switch port stays green as long as both the PC and IP Phone are authenticated. When the PC goes to sleep, or gets disconnected, the LED of the switch port changes to amber. If the PC is reconnected, then the LED changes back to green.

MDA does not enforce the order-of-device authentication. However, for best results, we recommend that a voice device is authenticated before a data device on an MDA-enabled port.

When you connect IP phones to a dot1x secured port, we recommend that you use MDA, instead of Cisco Discovery Protocol (CDP) bypass.

Note Any traffic destined to an unauthenticated client will be dropped. Traffic originating from an unauthenticated device will not be dropped.

Follow these guidelines for configuring MDA:

- To configure a switch port for MDA, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.
- You must configure the voice VLAN for the IP phone when the host mode is set to multi-domain. For more information, see the "Configuring VLANS" chapter of the *Catalyst 3750 Switch Software Configuration Guide, Release 12.2(58)SE*.
- To authorize a voice device, the AAA server must be configured to send a Cisco Attribute-Value (AV) pair attribute with a value of device-traffic-class=voice. Without this value, the switch treats the voice device as a data device.
- The guest VLAN and restricted VLAN features only apply to the data devices on an MDA-enabled port. The switch treats a voice device that fails authorization as a data device.
- If more than one device attempts authorization on either the voice or the data domain of a port, it is error disabled.
- Non-Cisco IP phones or voice devices are allowed into both the data and voice VLANs. The data VLAN allows the voice device to contact a DHCP server to obtain an IP address and acquire the voice VLAN information. After the voice device starts sending on the voice VLAN, its access to the data VLAN is blocked.
- A voice device MAC address that is binding on the data VLAN is not counted towards the port security MAC address limit.
- MDA can use MAC authentication bypass as a fallback mechanism to allow the switch port to connect to devices that do not support 802.1X authentication.
- When a data or a voice device is detected on a port, its MAC address is blocked until authorization succeeds. If the authorization fails, the MAC address remains blocked for five minutes.
- If more than five devices are detected on the data VLAN or more than one voice device is detected on the voice VLAN while a port is unauthorized, the port is error disabled.
- When a port host mode changes from single- or multihost to multidomain mode, an authorized data device remains authorized on the port. However, a Cisco IP phone on the port voice VLAN is automatically removed and must be reauthenticated on that port.

- Active fallback mechanisms such as guest VLAN and restricted VLAN remain configured after a port changes from single-host or multihost mode to multidomain mode.
- Switching a port host mode from multidomain to single-host or multiple-hosts mode removes all authorized devices from the port.
- If a data domain is authorized first and placed in the guest VLAN, non-802.1X-capable voice devices need their packets tagged on the voice VLAN to trigger authentication. The phone need not need to send tagged traffic. (The same is true for an 802.1X-capable phone.)
- It is not recommended to use per-user ACLs with an MDA-enabled port. An authorized device with a per-user ACL policy might impact traffic on both the port voice and data VLANs. You can use only one device on the port to enforce per-user ACLs.

How to Configure IEEE 802.1X Multidomain Authentication

Configuring IEEE 802.1X Multidomain Authentication

SUMMARY STEPS

1. **configure terminal**
2. **radius-server vsa send authentication**
3. **interface** *type slot/port*
4. **access-session host-mode multi-domain**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**radius-server vsa send authentication** **Example:** `Switch(config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes (VSAs).
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**access-session host-mode multi-domain** **Example:** `Switch(config-if)# access-session host-mode multi-domain`	Allows both a host and a voice device, such as an IP phone (Cisco or non-Cisco), to be authenticated on an 802.1X-authorized port. **Note** You must configure the voice VLAN for the IP phone when the host mode is set to multi-domain. See the "Configuring Voice VLAN" chapter of the *Catalyst 3750 Switch Software Configuration Guide, Release 12.2(58)SE* for more information. Make sure that the **authentication port-control** interface configuration command is set to **auto** for the specified interface.
Step 5	**exit** **Example:** `Switch(config)# exit`	Returns to privileged EXEC mode.

Configuring Critical Voice VLAN Support in Multidomain Authentication Mode

Perform this task on a port to configure critical voice VLAN support in multidomain authentication (MDA) mode.

Note To configure MDA mode, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **authentication event server dead action authorize vlan** *vlan-id*
5. **authentication event server dead action authorize voice**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet 0/1`	Specifies the port to be configured and enters interface configuration mode.
Step 4	**authentication event server dead action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event server dead action authorize vlan 40`	Configures a critical data VLAN. **Note** This step is only required if the **authentication event server dead action authorize vlan** *vlan-id* command is not configured on the port.
Step 5	**authentication event server dead action authorize voice** **Example:** `Switch(config-if)# authentication event server dead action authorize voice`	Enables the Critical Voice VLAN feature, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.

Configuration Examples for IEEE 802.1X Multidomain Authentication

Example: Configuring IEEE 802.1X Multidomain Authentication

The following example shows how to enable MDA and to allow both a host and a voice device on the port:

```
Device(config)interface GigabitEthernet0/0/0
Device(config-if)# switchport access vlan 110
Device(config-if)# switchport voice vlan 110
Device(config-if)# no ip address
Device(config-if)# authentication host-mode multi-domain
Device(config-if)# authentication port-control auto
Device(config-if)# mab
Device(config-if)# dot1x pae authenticator
Device(config-if)# end
```

Example: Critical Voice VLAN Support in Multidomain Authentication Mode

The following example shows how to enable the Critical Voice VLAN feature in MDA host-mode:

```
Switch(config) interface GigabitEthernet 0/0/0
Switch(config-if)# switchport access vlan 110
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# no ip address
Switch(config-if)# authentication event server dead action authorize vlan 12
Switch(config-if)# authentication event server dead action authorize voice
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication port-control auto
Switch(config-if)# mab
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

Additional References

Related Documents

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

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

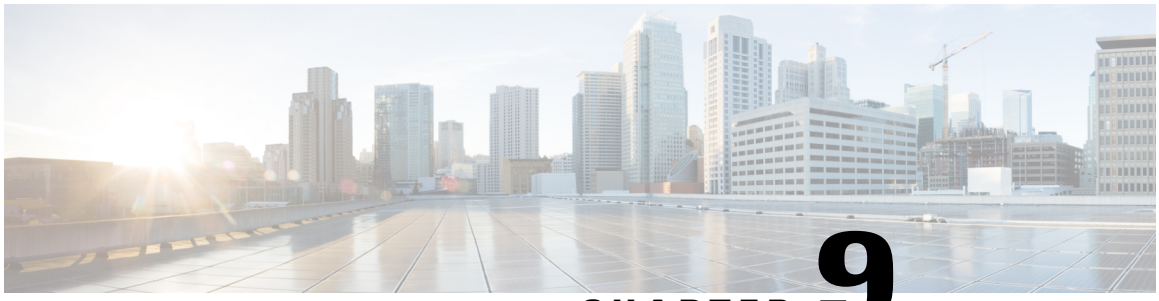
Feature Information for IEEE 802.1X Multidomain Authentication

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 10: Feature Information for IEEE 802.1X Multidomain Authentication

Feature Name	Releases	Feature Information
IEEE 802.1X Multidomain Authentication	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	Multi-domain authentication (MDA) allows both a data device and voice device, such as an IP phone (Cisco or non-Cisco), to authenticate on the same switch port. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 9

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.

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. **access-session 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:** `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	**dot1x system-auth-control** **Example:** `Device(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:** `Device(config)# interface Gigabitethernet 1/2/1`	Enters interface configuration mode.
Step 5	**switchport** **Example:** `Device(config-if)# switchport`	Places the interface in Layer 2-switched mode.
Step 6	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Sets a nontrunking, nontagged single VLAN Layer 2 interface.
Step 7	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 2`	Sets the VLAN for the port.
Step 8	**mab** [**eap**] **Example:** `Device(config-if)# mab`	(Optional) Enables MAB. • Enable MAB if the authentication order includes the **mab** keyword (see Step 11).
Step 9	**access-session port-control**{**auto**|**force-authorized**|**force unauthorized**} **Example:** `Device(config-if)# access-session port-control auto`	Configures the authorization state of the port.
Step 10	**authentication** *fallback profile* **Example:** `Device(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:** `Device(config-if)# authentication order mab dot1x webauth`	Configures the authentication order.
Step 12	**dot1x pae authenticator** **Example:** `Device(config-if)# dot1x pae authenticator`	Enables the port to respond to messages meant for an IEEE 802.1x authenticator.
Step 13	**end** **Example:** `Device(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 Gigabitethernet 1/2/1`	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

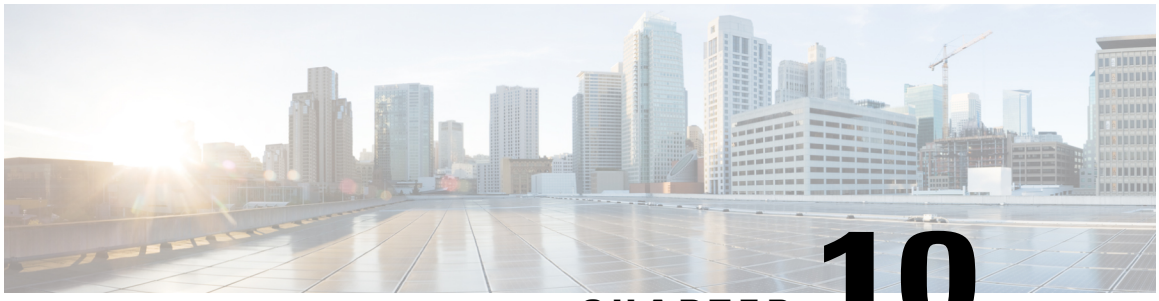
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 11: Feature Information for IEEE 802.1X Flexible Authentication

Feature Name	Releases	Feature Information
IEEE 8021.X Flexible Authentication	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	

Feature Name	Releases	Feature Information
		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. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers. 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**.



CHAPTER 10

IEEE 802.1X Open Authentication

IEEE 802.1X Open Authentication allows a host to have network access without having to go through IEEE 802.1X authentication. Open authentication is useful in an applications such as the Preboot Execution Environment (PXE), where a device must access the network to download a bootable image containing an authentication client.

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 Open 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.

The switch must be connected to a Cisco secure Access Control System (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 IEEE 802.1X Open Authentication

- This feature does not support standard ACLs on the switch port.
- If you configure Open Authentication by using the **authentication open** interface configuration command, any new MAC address detected on the port will be allowed unrestricted Layer 2 access to the network even before any authentication has succeeded. If you use this command, you should use static default ACLs to restrict Layer 3 traffic.
- The Network Edge Access Topology (NEAT) feature is not supported with IEEE 802.1X Open Authentication.

Information About IEEE 802.1X Open Authentication

IEEE 802.1X Open Authentication and Host Modes

Any of the four host modes (single-host mode, multiple-host mode, multi-domain authentication mode, and multiauthentication mode) may be configured to allow a device to gain network access before authentication. For information about configuring IEEE 802.1X host modes, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

Open authentication is enabled by entering the **authentication open** command after host mode configuration, and acts as an extension to the configured host mode. For example, if open authentication is enabled with single-host mode, then the port will allow only one MAC address. When preauthentication open access is enabled, initial traffic on the port is restricted only by whatever other access restriction, independent of 802.1X, is configured on the port. If no access restriction other than 802.1X is configured on the port, then a client device will have full access on the configured VLAN.

How to Configure IEEE 802.1X Open Authentication

Configuring IEEE 802.1X Open Authentication

Before You Begin

Note To configure open authentication you must have configured one of the four 802.1X host modes. For information about configuring IEEE 802.1X host modes, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **access-session port-control auto**
4. **access-session host-mode** {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**]
5. **access-session open**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode. 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	**access-session port-control auto** **Example:** `Switch(config-if)# access-session port-control auto`	Enables port-based authentication on the interface.
Step 4	**access-session host-mode** {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**] **Example:** `Switch(config-if)# access-session host-mode single-host`	Configures the host mode (single-host mode, multiple-host mode, multidomain authentication mode, and multiauthentication mode) on the authorized port or allows open access (no access restrictions).
Step 5	**access-session open** **Example:** `Switch(config-if)# access-session open`	Enables open authentication. **Note** This command overrides the **authentication host-mode** {**single-host** | **multi-auth** | **multi-domain** | **multi-host**} [**open**] command for the port only.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for IEEE 802.1X Open Authentication

Example: Configuring IEEE 802.1X Open Authentication

The following example shows how to enable the Open Authentication feature on a port that has been configured in single-host mode:

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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*
Configuring host modes	"Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

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

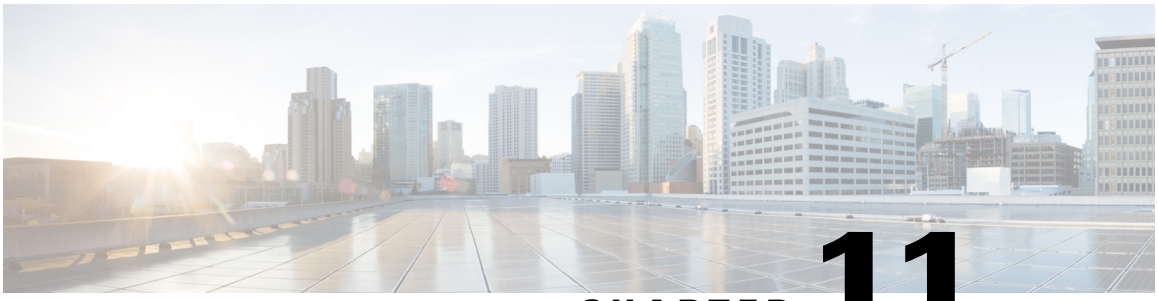
Feature Information for IEEE 802.1X Open Authentication

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 12: Feature Information for IEEE 802.1X Open Authentication

Feature Name	Releases	Feature Information
IEEE 802.1X Open Authentication	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	IEEE 802.1X Open Authentication allows a host to have network access without having to go through IEEE 802.1X authentication. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 11

IEEE 802.1X Auth Fail VLAN

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

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 Auth Fail VLAN

Host Mode

Before you configure auth fail VLAN, the switch need to be in single-host mode (see the see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(58)SE*.

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 Access Control System (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 IEEE 802.1X Auth Fail VLAN

- Auth fail VLANs are supported only on 802.1X ports in single-host mode and on Layer 2 ports.
- The auth fail VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.
- This feature does not support standard ACLs on the switch port.
- You can configure any active VLAN except a remote SPAN (RSPAN) VLAN, a primary private VLAN, or a voice VLAN as an 802.1X auth fail VLAN.

Information About IEEE 802.1X Auth Fail VLAN

802.1X Authentication with Auth Fail VLAN

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

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

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

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

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

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

Note Auth fail VLANs are supported only on 802.1X ports in single-host mode and on Layer 2 ports.

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

Other security features such as dynamic ARP Inspection, DHCP snooping, and IP source guard can be configured independently on an auth fail VLAN.

How to Configure IEEE 802.1X Auth Fail VLAN

Configuring an IEEE 802.1X Auth Fail VLAN

Perform this optional task to configure an auth fail VLAN.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **access-session port-control auto**
4. **authentication event fail action authorize vlan** *vlan-id*
5. **end**
6. **show access-session interface** *interface-id*
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode. For the supported port types, see the "802.1X Authentication Configuration Guidelines" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(58)SE*.
Step 3	**access-session port-control auto** **Example:** `Switch(config-if)# access-session port-control auto`	Enables 802.1X authentication on the port.
Step 4	**authentication event fail action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event fail action authorize vlan 40`	Specifies an active VLAN as an 802.1X auth fail VLAN. The range is 1 to 4094.

	Command or Action	Purpose
Step 5	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show access-session interface** *interface-id* **Example:** `Switch# show access-session interface gigabitethernet0/1`	(Optional) Verify your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

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

Configuring the Number of Authentication Retries

You can configure the maximum number of authentication attempts allowed before a user is assigned to the restricted VLAN by using the **authentication event retry** *retry count* interface configuration command. The range of allowable authentication attempts is 1 to 3. The default is 3 attempts.

Perform this optional task to configure the maximum number of allowed authentication attempts.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **access-session port-control auto**
4. **authentication event fail action authorize vlan** *vlan-id*
5. **authentication event failretry** *retry-count*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode. For the supported port types, see the "802.1X Authentication Configuration Guidelines" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter in the *Catalyst 3750 Switch Software Configuration Guide, 12.2(58)SE*.
Step 3	**access-session port-control auto** **Example:** `Switch(config-if)# access-session port-control auto`	Enables 802.1X authentication on the port.
Step 4	**authentication event fail action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event fail action authorize vlan 40`	Specifies an active VLAN as an 802.1X auth fail VLAN. The range is 1 to 4094.
Step 5	**authentication event failretry** *retry-count* **Example:** `Switch(config-if)# authentication event fail retry 4`	Specifies a number of authentication attempts before a port moves to the auth fail VLAN. The range is 0 to 5, and the default is 2 attempts after the initial failed event.
Step 6	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.

Example

The following example shows how to set 2 as the number of authentication attempts allowed before the port moves to the auth fail VLAN:

```
Switch(config-if)# authentication event retry 2
```

Configuration Examples for IEEE 802.1X Auth Fail VLAN

Example: Configuring IEEE 802.1X Auth Fail VLAN

The following example shows how to enable VLAN 2 as an 802.1X auth fail VLAN:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# authentication port-control auto
Switch(config-if)# authentication event fail action authorize 2
```

Example: Configuring the Number of Authentication Retries

The following example specifies that after three failed authentication attempts the port is assigned to an auth fail VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# authentication event fail retry 3 action authorize vlan 40
Switch(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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*
Configuring host modes	"Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter

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

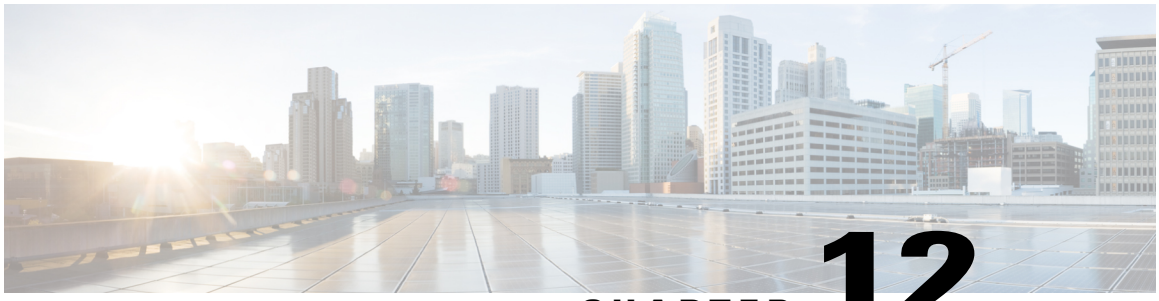
Feature Information for IEEE 802.1X Auth Fail VLAN

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 13: Feature Information for IEEE 802.1X Auth Fail VLAN

Feature Name	Releases	Feature Information
IEEE 802.1X Auth Fail VLAN	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	An auth fail VLAN allows users without valid credentials in an authentication server to access a limited set of services. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 12

Critical Voice VLAN Support

Critical Voice VLAN Support puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.

With normal network connectivity, when an IP phone successfully authenticates on a port, the authentication server puts the phone into the voice domain. If the authentication server becomes unreachable, IP phones cannot authenticate. In multidomain authentication (MDA) mode or multiauthentication mode, you can configure the Critical Voice VLAN support feature to put phone traffic into the configured voice VLAN of 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.

Restrictions for Critical Voice VLAN Support

- Use different VLANs for voice and data.

- The voice VLAN must be configured on the switch.
- ACLs are not supported on fixed Cisco Integrated Services Routers (ISRs).
- This feature does not support standard ACLs on the switch port.

Information About Critical Voice VLAN Support

Critical Voice VLAN Support in Multidomain Authentication Mode

If a critical voice VLAN is deployed using an interface in multidomain authentication (MDA) mode, the host mode is changed to multihost and the first phone device is installed as a static forwarding entries. Any additional phone devices are installed as dynamic forwarding entry in the Host Access Table (HAT).

For further information about host modes, see the *802.1X Authentication Services Configuration Guide*.

Note If a critical port is already authorized and reauthentication occurs, the switch puts the port in the critical-authentication state in the current VLAN, which might be the one previously assigned by the RADIUS server.

Note Inaccessible authentication bypass is compatible with guest VLAN. When a guest VLAN is enabled on a 802.1X port, the features interact as follows: if all RADIUS servers are not available and if a client is connected to a critical port and was previously assigned to a guest VLAN, the switch keeps the port in the guest VLAN.

Critical Voice VLAN Support in Multiauthentication Mode

If the critical authentication feature is deployed in multiauthentication mode, only one phone device will be allowed and a second phone trying to authorize will trigger a violation.

The **show authentication sessions** command displays the critical voice client data. A critically authorized voice client in multiauthentication host mode will be in the “authz success” and “authz fail” state.

Note If critical voice is required, then critical data should be configured too. Otherwise, the critical voice client will be displayed in the “authz fail” state while the voice VLAN will be open.

How to Configure Critical Voice VLAN Support

Configuring Critical Voice VLAN Support in Multidomain Authentication Mode

Perform this task on a port to configure critical voice VLAN support in multidomain authentication (MDA) mode.

Note To configure MDA mode, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **authentication event server dead action authorize vlan** *vlan-id*
5. **authentication event server dead action authorize voice**

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.
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet 0/1`	Specifies the port to be configured and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**authentication event server dead action authorize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event server dead action authorize vlan 40`	Configures a critical data VLAN. **Note** This step is only required if the **authentication event server dead action authorize vlan** *vlan-id* command is not configured on the port.
Step 5	**authentication event server dead action authorize voice** **Example:** `Switch(config-if)# authentication event server dead action authorize voice`	Enables the Critical Voice VLAN feature, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.

Configuring Critical Voice VLAN Support in Multiauthentication Mode

Perform this task to configure critical voice VLAN support in multiauthentication mode.

Note To configure multiauthentication mode, see the "Configuring the Host Mode" section of the "Configuring IEEE 802.1X Port-Based Authentication" chapter.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **authentication event server dead action reinitialize vlan** *vlan-id*
5. **authentication event server dead action authorize voice**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet 0/1`	Specifies the port to be configured and enters interface configuration mode.
Step 4	**authentication event server dead action reinitialize vlan** *vlan-id* **Example:** `Switch(config-if)# authentication event server dead action reinitialize vlan 40`	Configures a critical data VLAN. **Note** This step is only required if the **authentication event server dead action authorize vlan** *critical-data-vlan-id* command is not configured on the port.
Step 5	**authentication event server dead action authorize voice** **Example:** `Switch(config-if)# authentication event server dead action authorize voice`	Enables the Critical Voice VLAN support feature, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable.

Configuration Examples for Critical Voice VLAN Support

Example: Critical Voice VLAN Support in Multidomain Authentication Mode

The following example shows how to enable the Critical Voice VLAN feature in MDA host-mode:

```
Switch(config) interface GigabitEthernet 0/0/0
Switch(config-if)# switchport access vlan 110
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# no ip address
Switch(config-if)# authentication event server dead action authorize vlan 12
Switch(config-if)# authentication event server dead action authorize voice
Switch(config-if)# authentication host-mode multi-domain
Switch(config-if)# authentication port-control auto
Switch(config-if)# mab
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

Example: Critical Voice VLAN Support in Multiauthentication Mode

The following example shows how to enable the Critical Voice VLAN support feature in multiauthentication mode:

```
Switch(config) interface GigabitEthernet 0/0/0
Switch(config-if)# switchport access vlan 110
Switch(config-if)# switchport voice vlan 110
Switch(config-if)# no ip address
Switch(config-if)# authentication event server dead action reinitialize vlan 12
Switch(config-if)# authentication event server dead action authorize voice
Switch(config-if)# authentication host-mode multi-auth
Switch(config-if)# authentication port-control auto
Switch(config-if)# mab
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# end
```

Additional References

Related Documents

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

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 Critical Voice VLAN Support

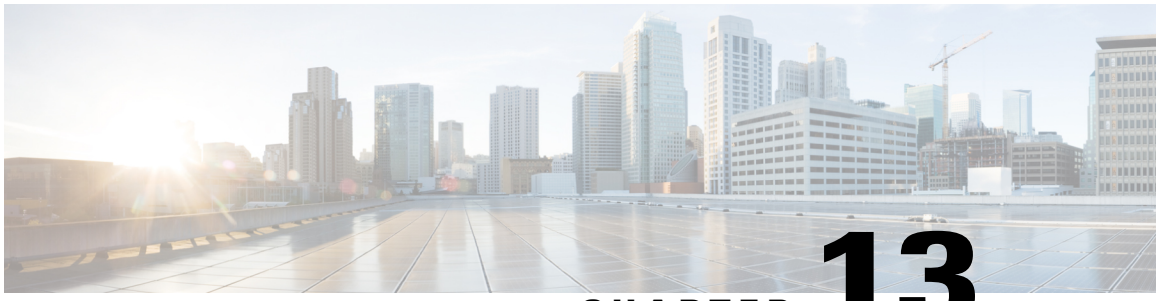
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 14: Feature Information for Critical Voice VLAN Support

Feature Name	Releases	Feature Information
Critical Voice VLAN Support	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	This feature enables critical voice VLAN support, which puts phone traffic into the configured voice VLAN of a port if the authentication server becomes unreachable. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.

Feature Name	Releases	Feature Information
Critical VLAN with Multi-auth	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	This feature adds support for the Critical Voice VLAN feature in multiauthentication mode. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 13

IEEE 802.1X Wake on LAN Support

The IEEE 802.1X Wake on LAN (WoL) Support feature allows dormant PCs to be powered up when the switch receives a specific Ethernet frame, known as the "magic packet." You can use this feature in environments where administrators need to connect to systems that have been powered down.

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 Wake on LAN Support

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 Access Control Sytem (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 IEEE 802.1X Wake on LAN Support

- WoL is supported only on ports configured in 802.1X single-host, multihost and multidomain modes.
- It is supported only on ports configured for PortFast. See the “Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard” module for further information.
- It is supported only in 802.1X AUTO modes.
- WoL is supported only on Cisco 88x/89x/86x routers and High Speed Wan interface cards (HWIC).
- This feature does not support standard ACLs on the switch port.

Information About IEEE 802.1X Wake on LAN Support

IEEE 802.1X Authentication with Wake on LAN

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

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

When the switch uses 802.1X authentication with WoL, the switch forwards traffic to unauthorized 802.1x ports, including magic packets. While the port is unauthorized, the switch continues to block ingress traffic

other than EAPOL packets. The host can receive packets but cannot send packets to other devices in the network.

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

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

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

How to Configure IEEE 802.1X Wake on LAN Support

Configuring IEEE 802.1X Authentication with Wake on LAN

Perform this task to enable 802.1X authentication with WoL. This procedure is optional.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type slot/port*
3. **access-session control-direction** {**both** | **in**}
4. **end**
5. **show authentication interface** *interface-id*
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type slot/port* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to which multiple hosts are indirectly attached, and enters interface configuration mode.

	Command or Action	Purpose
Step 3	**access-session control-direction** {**both** | **in**} **Example:** `Switch(config-if)# access-session control-direction both`	Enables 802.1X authentication with WoL on the port. Use these keywords to configure the port as bidirectional or unidirectional: • **both—**Sets the port as bidirectional. The port cannot receive packets from or send packets to the host. By default, the port is bidirectional. • **in—**Sets the port as unidirectional. The port can send packets to the host but cannot receive packets from the host.
Step 4	**end** **Example:** `Switch(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**show authentication interface** *interface-id* **Example:** `Switch# show authentication interface gigabitethernet0/1`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuration Examples for IEEE 802.1X Wake on LAN Support

Example: Configuring IEEE 802.1X Wake on LAN Support

The following example shows how to enable 802.1X authentication with WoL and sets the port as bidirectional:

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# authentication control-direction both
```

Additional References

Related Documents

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

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

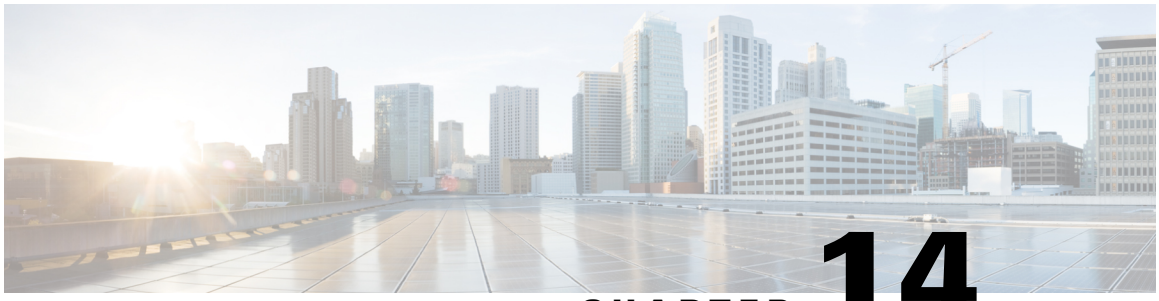
Feature Information for IEEE 802.1X Wake on LAN Support

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 15: Feature Information for IEEE 802.1X Wake on LAN Support

Feature Name	Releases	Feature Information
IEEE 802.1X Wake on LAN Support	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	The 802.1X authentication with the Wake on LAN (WoL) feature allows dormant PCs to be powered up when the switch receives a specific Ethernet frame, known as the “magic packet.” In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.



CHAPTER 14

Per-User ACL Support for 802.1X/MAB/Webauth Users

This feature allows per-user ACLs to be downloaded from the Cisco Access Control Server (ACS) as policy enforcement after authentication using IEEE 802.1X, MAB authentication bypass, or web authentication.

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.

PrerequisitesforPer-UserACLSupportfor802.1X/MAB/Webauth Users

- AAA authentication must be enabled.

- AAA authorization must be enabled by using the **network** keyword to allow interface configuration from the RADIUS server.
- 802.1X authentication must be enabled.
- The user profile and VSAs must be configured on the RADIUS server.

Restrictions for Per-User ACL Support for 802.1X/MAB/Webauth Users

- Per-user Access Control Lists (ACLs) are supported only in single-host mode.
- This feature does not support standard ACLs on the switch port.
- Only one 802.1X-authenticated user is supported on a port. If the multiple-hosts mode is enabled on the port, the per-user ACL attribute is disabled for the associated port.
- The maximum size of the per-user ACL is 4000 ASCII characters but is limited by the maximum size of RADIUS-server per-user ACLs.
- ACLs are not supported on fixed Cisco Integrated Services Routers (ISRs).

Information About Per-User ACL Support for 802.1X/MAB/Webauth Users

802.1X Authentication with Per-User ACLs

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

Router ACLs and input port ACLs can be confiugured on the same switch. However, a port ACL takes precedence over a router ACL. If an input port ACL is applied to an interface that belongs to a VLAN, the port ACL takes precedence over an input router ACL that is applied to the VLAN interface. Incoming packets received on the port to which a port ACL is applied are filtered by the port ACL. Incoming routed packets received on other ports are filtered by the router ACL. Outgoing routed packets are filtered by the router ACL. To avoid configuration conflicts, the user profiles should be carefully planned and stored on the RADIUS server.

RADIUS supports per-user attributes, including vendor-specific attributes. These vendor-specific attributes (VSAs) are in octet-string format and are passed to the switch during the authentication process. The VSAs used for per-user ACLs are inacl#<n > for the ingress direction and outacl#<n > for the egress direction. MAB ACLs are supported only in the ingress direction. The switch supports VSAs only in the ingress direction. It

does not support port ACLs in the egress direction on Layer 2 ports. For more information, see the "Configuring Network Security with ACLs|" module.

The extended ACL syntax style should be used to define the per-user configuration that is stored on the RADIUS server. When the definitions are passed from the RADIUS server, they are created by using the extended naming convention. However, if the Filter-Id attribute is used, it can point to a standard ACL.

The Filter-Id attribute can be used to specify an inbound or outbound ACL that is already configured on the switch. The attribute contains the ACL number followed by *.in* for ingress filtering or *.out* for egress filtering. If the RADIUS server does not allow the *.in* or *.out* syntax, the access list is applied to the outbound ACL by default. Because of limited support of Cisco IOS access lists on the switch, the Filter-Id attribute is supported only for IP ACLs numbered 1 to 199 and 1300 to 2699 (IP standard and IP extended ACLs).

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

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

How to Configure Per-User ACL Support for 802.1X/MAB/Webauth Users

Configuring Downloadable ACLs

To configure a switch to accept downloadable ACLs or redirect URLs from the RADIUS server during authentication of an attached host, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip device tracking**
4. **aaa new-model**
5. **aaa authorization network default group radius**
6. **radius-server vsa send authentication**
7. **interface** *interface-id*
8. **ip access-group** *acl-id* **in**
9. end
10. **show running-config interface***interface-id*
11. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted .
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ip device tracking** **Example:** `Switch(config)# ip device tracking`	Enables the IP device tracking table.
Step 4	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables AAA.
Step 5	**aaa authorization network default group radius** **Example:** `Switch(config)# aaa authorization network default group radius`	Sets the authorization method. To remove the authorization method, use the **no aaa authorization network default group radius** command.
Step 6	**radius-server vsa send authentication** **Example:** `Switch(config)# radius-server vsa send autentication`	Configures the network access server.
Step 7	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet0/1`	Specifies the port to be configured, and enters interface configuration mode.
Step 8	**ip access-group** *acl-id* **in** **Example:** `Switch(config-if)# ip access-group 99 in`	Configures the default ACL on the port in the input direction. **Note** The ACL ID is an access list name or number.
Step 9	end	`Switch(config-if)# end` Returns to Privileged EXEC mode.
Step 10	**show running-config interface***interface-id* **Example:** `Switch# show running-config interface interface-id`	Displays the specific interface configuration for verification.

	Command or Action	Purpose
Step 11	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Save entries in the configuration file.

Configuration Examples for Per-User ACL Support for 802.1X/MAB/Webauth Users

Example: Configuring a Switch for a Downloadable Policy

The following example shows how to configure a switch for a downloadable policy:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local group radius
Switch(config)# ip device tracking
Switch(config)# ip access-list extended default_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# radius-server vsa send authentication
Switch(config)# interface fastEthernet 2/13
Switch(config-if)# ip access-group default_acl in
Switch(config-if)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Authentication commands	*Cisco IOS Security Command Reference Commands A to C*
IPsec	*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 15.0.*
RADIUS	“Configuring RADIUS” module.
Standalone MAB Support	*Standalone MAB Support*
Layer 2 ports	Configuring Network Security with ACLs

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–MAB–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 Per-User ACL Support for 802.1X/MAB/Webauth Users

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 16: Feature Information for Per-User ACL Support for 802.1X/MAB/Webauth Users

Feature Name	Releases	Feature Information
Per-User ACL Support for 802.1X/MAB/Webauth Users	Cisco IOS XE 3.2SE Cisco IOS XE 3.3SE Cisco IOS XE Release 3.6E	This feature allows per-user ACLs to be downloaded from the Cisco Access Control Server (ACS) as policy enforcement after authentication using IEEE 802.1X, MAB authentication bypass, or web authentication. In Cisco IOS XE Release 3.2SE, this feature was supported on the following platforms: • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller In Cisco IOS XE Release 3.3SE, this feature was supported on the following platforms: • Catalyst 3650 Series Switches • Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. In Cisco IOS XE Release 3.3SE, this feature is supported on Cisco 5700 Wireless LAN Controllers.