



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, page 1](#)
- [Prerequisites for IEEE 802.1X Voice VLAN, page 1](#)
- [Restrictions for IEEE 802.1X Voice VLAN, page 3](#)
- [Information About IEEE 802.1X Voice VLAN, page 4](#)
- [How to Configure IEEE 802.1X Voice VLAN, page 5](#)
- [Configuration Example for IEEE 802.1X Voice VLAN, page 7](#)
- [Additional References for IEEE 802.1X Port-Based Authentication, page 7](#)
- [Feature Information for IEEE 802.1X Voice VLAN, page 8](#)

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 <i>interface-id</i> 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 fastethernet 1/0 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#
```

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	<i>Port Based Network Access Control</i>
RFC 3580	<i>IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines</i>

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 <http://www.cisco.com/go/featurenavigator>. An account on Cisco.com is not required.

Table 1: 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	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 is supported on Cisco 5700 Wireless LAN Controllers.

