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 1: 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.