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 1: 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.