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, page 1
- Prerequisites for IEEE 802.1X Open Authentication, page 2
- Restrictions for IEEE 802.1X Open Authentication, page 2
- Information About IEEE 802.1X Open Authentication, page 3
- How to Configure IEEE 802.1X Open Authentication, page 3
- Configuration Examples for IEEE 802.1X Open Authentication, page 5
- Additional References, page 5
- Feature Information for IEEE 802.1X Open Authentication, page 6

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 1: 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	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 is supported on Cisco 5700 Wireless LAN Controllers.