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 1: 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	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 is supported on Cisco 5700 Wireless LAN Controllers.