Release Notes for the Catalyst 2960 Switches, Cisco IOS Release 12.2(37)EY

August 8, 2007

Cisco IOS Releases 12.2(37)EY runs only on Catalyst 2960 switches that support the LAN Lite image. For information on other releases of the Catalyst 2960 switches, see the *Release Notes for the Catalyst 3750, 3560, 2970, and 2960 Switches, Cisco IOS Release 12.2(37)SE and later*.

These release notes include important information about Cisco IOS Release 12.2(37)EY and any limitations, restrictions, and caveats that apply to this release. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 4.

Cisco IOS Release 12.2(37)EY is based on Cisco IOS Release 12.2(37)SE. Open caveats in Cisco IOS Release 12.2(37)SE also affect Cisco IOS Release 12.2(37)EY, unless they are listed in the Cisco IOS Release 12.2(37)EY resolved caveats list. The list of open caveats in Cisco IOS Release 12.2(37)SE is available at this URL:

http://www.cisco.com/en/US/products/hw/switches/ps5023/prod_release_note09186a0080838bbf.html

For the complete list of Catalyst 2960 switch documentation, see the "Related Documentation" section on page 16.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

This information is in the release notes:

System Requirements

The system requirements are described in these sections:

Hardware Supported

Table 1 lists the hardware supported on this release.

Table 1 Catalyst 2960 Switch Supported Hardware

Switch	Description
Catalyst 2960-24-S	24 10/100BASE-TX Ethernet ports
Catalyst 2960-24TC-S	24 10/100BASE-TX Ethernet ports and 2 dual-purpose uplinks[1] (two 10/100/1000BASE-T copper ports and two SFP[2] module slots)
Catalyst 2960-48TC-S	48 10/100BASE-TX Ethernet ports and 2 dual-purpose uplinks1 (two 10/100/1000BASE-T copper ports and two SFP module slots)

1. Each uplink port is considered a single interface with dual front ends (RJ-45 connector and SFP module slot). The dual front ends are not redundant interfaces, and only one port of the pair is active.
2. SFP = small form-factor pluggable.

Device Manager System Requirements

These sections describes the hardware and software requirements for using the device manager:

- "Hardware Requirements" section on page 3
- "Software Requirements" section on page 3

Hardware Requirements

Table 2 lists the minimum hardware requirements for running the device manager.

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II[1]	64 MB[2]	256	1024 x 768	Small

1. We recommend Intel Pentium 4.
2. We recommend 256-MB DRAM.

Software Requirements

Table 3 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.

Note The device manager does not require a plug-in.

Table 3 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer[1]	Mozilla Firefox
Windows 2000	None	5.5, 6.0 or 7.0	1.5
Windows XP	None	5.5, 6.0 or 7.0	1.5

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI) or the Network Assistant application.

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 2960 switch, all standby command switches must be Catalyst 2960 switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant* and *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com), the software configuration guide, the command reference, and the Cisco EtherSwitch service module feature guide.

CNA Compatibility

Cisco IOS 12.2(37)EY is only compatible with Cisco Network Assistant (CNA) 5.2 and later. You can download Cisco Network Assistant from this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- "Finding the Software Version and Feature Set" section on page 4
- "Deciding Which Files to Use" section on page 4
- "Upgrading a Switch by Using the Device Manager or Network Assistant" section on page 5
- "Upgrading a Switch by Using the CLI" section on page 5
- "Recovering from a Software Failure" section on page 6

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

These are the Cisco IOS Software image files for the Catalyst 2960 switch:

c2960-lanbase-tar.122-37.EY.tar	Catalyst 2960 image file and device manager files. This image has Layer 2+ features.
c2960-lanbasek9-tar.122-37.EY.tar	Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features.

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. For detailed instructions, click **Help**.

Note When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

Step 1 Identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

To download the image for a Catalyst 2960 switch, click **Catalyst 2960 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2960 3DES Cryptographic Software**.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, see Appendix B in the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For **//***location*, specify the IP address of the TFTP server.

For */directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/c2960-ipservices-tar.122-37.EY.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For additional recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Features

These sections describe the new supported hardware and the new and updated software features provided in this release:

- "New Hardware Features" section on page 7
- "New Software Features" section on page 7

New Hardware Features

For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

This release is the first software release for the Catalyst 2960 switches with LAN Lite software. For a detailed list of features for this software release, refer to the *Catalyst 2960 Switch LAN Lite Software Configuration Guide*.

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

This section contains these limitations:

- "Cisco IOS Limitations" section on page 8
- "Device Manager Limitations" section on page 10

Cisco IOS Limitations

These limitations apply to the Catalyst 2960 switch:

- "Configuration" section on page 8
- "Ethernet" section on page 9
- "IP Telephony" section on page 9
- "SPAN" section on page 9
- "SPAN" section on page 9
- "Trunking" section on page 10
- "Trunking" section on page 10
- "VLAN" section on page 10

Configuration

These are the configuration limitations:

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted up without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs if a crypto key is generated after an SSL client session.

  There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

Ethernet

These are the Ethernet limitations:

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

  If this happens, uneven traffic distribution will happen on EtherChannel ports.

  Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

  - for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
  - for incrementing source-ip traffic, configure load balance method as **src-ip**
  - for incrementing dest-ip traffic, configure load balance method as **dst-ip**
  - Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

  For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

IP Telephony

These are the IP telephony limitations:

- Some access point devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These access points should be discovered as Cisco pre-standard devices. The **show power inline** user EXEC command shows the access point as an IEEE Class 1 device. The workaround is to power the access point by using an AC wall adaptor. (CSCin69533)
- After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)
- The Cisco 7905 IP Phone is error-disabled when the phone is connected to wall power.

  The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

SPAN

This is the SPAN limitation.

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Trunking

These are the trunking limitations:

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

VLAN

This is the VLAN limitation:

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

Device Manager Limitations

These are the device manager limitations:

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

  The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

Important Notes

These sections describe the important notes related to this software release for the Catalyst 2960 switch:

- "Cisco IOS Notes" section on page 11
- "Device Manager Notes" section on page 11

Cisco IOS Notes

This note applies to Cisco IOS software:

- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  If this message appears, check that there is network connectivity between the switch and the ACS. You should also check that the switch has been properly configured as an AAA client on the ACS.

Device Manager Notes

These notes apply to the device manager:

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese
- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

  From Microsoft Internet Explorer:

  1. Choose **Tools** > **Internet Options**.
  2. Click **Settings** in the “Temporary Internet files” area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

- The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

  If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

  If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configure the HTTP server interface for the type of authentication that you want to use. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used. • **tacacs**—TACACS server is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.cisco.com:84*), you must enter *http://* as the URL prefix. Otherwise, you cannot launch the device manager.

Open Caveats

This section describes the open caveats in this software release:

- CSCsb85001

  If traffic is passing through VMPS ports and you perform a **shut** operation, a dynamic VLAN is not assigned and a VLAN with a null ID appears.

  The workaround is to clear the MAC address table. This forces the VMPS server to correctly reassign the VLAN.

- CSCsc96474

  The switch might display tracebacks similar to these examples when a large number of IEEE 802.1x supplicants try to repeatedly log in and log out.

  Examples:

  ```
  Jan 3 17:54:32 L3A3 307: Jan 3 18:04:13.459: %SM-4-BADEVENT: Event 'eapReq' is invalid
  for the current state 'auth_bend_idle': dot1x_auth_bend Fa9
  ```

  ```
  Jan 3 17:54:32 L3A3 308: -Traceback= B37A84 18DAB0 2FF6C0 2FF260 8F2B64 8E912C Jan 3
  19:06:13 L3A3 309: Jan 3 19:15:54.720: %SM-4-BADEVENT: Event 'eapReq_no_reAuthMax' is
  invalid for the current ate 'auth_restart': dot1x_auth Fa4
  ```

  ```
  Jan 3 19:06:13 L3A3 310: -Traceback= B37A84 18DAB0 3046F4 302C80 303228 8F2B64 8E912C
  Jan 3 20:41:44 L3A3 315: .Jan 3 20:51:26.249: %SM-4-BADEVENT: Event 'eapSuccess' is
  invalid for the current state 'auth_restart': dot1x_auth Fa9
  ```

  ```
  Jan 3 20:41:44 L3A3 316: -Traceback= B37A84 18DAB0 304648 302C80 303228 8F2B64 8E912C
  ```

  There is no workaround.

- CSCsd03580

  When IEEE 802.1x is globally disabled on the switch by using the **no dot1x system-auth-control** global configuration command, some interface level configuration commands, including the **dot1x timeout command**, become unavailable.

  The workaround is to enable the **dot1x system-auth-control** global configuration command before attempting to configure interface level IEEE 802.1x parameters.

  on command to the configuration and re-establishes communication with the RADIUS server.

- CSCse06827
- The switch might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.

  The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem.

- CSCsg79506

  During repeated reauthentication of supplicants on an IEEE 802.1x-enabled switch, if the RADIUS server is repeatedly going out of service and then coming back up, the available switch memory might deplete over time, eventually causing the switch to shut down.

  There is no work-around, except to ensure that the RADIUS server is stable.

- CSCsg81334

  If IEEE 802.1x critical authentication is not enabled and the RADIUS authentication server is temporarily unavailable during a reauthentication, when the RADIUS server comes back up, MAC authentication bypass (MAB) does not authenticate a previously authenticated client.

The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** command on the port connected to the client. An alternative, to prevent the problem from occurring, is to enable critical authentication by entering the **dot1x critical** {**eapol** | **recovery delay** *milliseconds*} global configuration command.

- CSCsi26392

  When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port.

- CSCsi26444

  The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:

  – IEEE 802.1 is enabled.

  – A supplicant is authenticated on at least one port.

  – A new member joins a switch stack.

  You can use one of these workarounds:

  – Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.

  – Remove and reconfigure the VLAN.

- CSCsi52707

  When setting an interface to its default configuration by using the **default** command, or when clearing the 802.1X mac-auth-bypass configuration from a port that was never authenticated, this message might appear:

  ```
  01:18:09: %SM-4-STOPPED: Event 'mabAbort' ignored because the state machine is
  stopped: dot1x_auth_mab -Traceback= 1D2368 3C1BA8 3C1D40 3C16A8 9EF8D8 9E6CC4
  ```

  There is no workaround. This message is only information, switch functionality is not affected.

- CSCsi75246

  An address learned as a supplicant that is aged out by port security aging is never relearned by port security under any of these conditions:

  – IEEE 802.1x authentication, port security, and port security aging are enabled on a port.

  – An address is cleared by port security.

  – You enter the **clear port security** privileged EXEC command.

  The workaround is to use the **dot1x timeout** interface configuration command instead of the port security aging timer as the reauthentication timer for IEEE 802.

- CSCsj04337

  You receive an Invalid Certificate error message when you start the Cisco Device Manager from a Firefox web browser.

  There is no workaround.

- CSCsj42841

  You cannot start a Telnet session from the Cisco Device Manager from an Internet Explorer 7.0 web browser.

  The workaround is to start a Telnet session from the command-line prompt.

Resolved Caveats

This section describes the resolved caveats in this software release:

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

- CSCsg70474

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsi60004

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

Related Documentation

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the URL referenced in the Obtaining Documentation, Obtaining Support, and Security Guidelines section.

These documents provide complete software information about the Catalyst 2960 switch that supports the LAN Lite Image:

- *Catalyst 2960 Switch Software Configuration Guide for the LAN Lite Image* (not orderable but available on Cisco.com)

  http://www.cisco.com/en/US/products/ps6406/products_configuration_guide_book09186a0080892a54.html

- *Catalyst 2960 Switch Command Reference for the LAN Lite Image* (not orderable but available on Cisco.com)

  http://www.cisco.com/en/US/products/ps6406/products_command_reference_book09186a008088e095.html

These documents provide complete information about other Catalyst 2960 switches:

- *Catalyst 2960 Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750, 3560, 3550, 2970, and 2960 Switch System Message Guide* (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide* (order number DOC-7816879=)

Note The above getting started guide, orderable in print, provides information in all supported languages. Listed below are online-only getting started guides in the individual languages.

- *Catalyst 2960 Switch Getting Started Guide*—English (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—Chinese (Simplified) (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—French (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—German (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—Italian (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—Japanese (not orderable but available on Cisco.com)
- *Catalyst 2960 Switch Getting Started Guide*—Spanish (not orderable but available on Cisco.com)

- *Regulatory Compliance and Safety Information for the Catalyst 2960 Switch* (order number DOC-7816880=)

For other information about related products, see these documents:

- Device manager online help (available on the switch)
- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Cisco RPS 300 Redundant Power System Hardware Installation Guide* (order number DOC-7810372=)
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide* (order number DOC-7815201=)
- For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

  - *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)
  - *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix* (not orderable but available on Cisco.com)
  - *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (not orderable but available on Cisco.com)
  - *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules* (not orderable but available on Cisco.com)

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html