Release Notes for Catalyst 2360 Switch, Cisco IOS Release 12.2(53)EY

June 22, 2010

Cisco IOS Release 12.2(53)EY runs on all Catalyst 2360 switches.

These release notes include important information about Cisco IOS Release 12.2(53)EY and any limitations, restrictions, and caveats that apply to it. 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 3.
- 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.

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

http://www.cisco.com/cisco/web/download/index.html

This software release is part of a special release of Cisco IOS software that is not released on the same 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.

Contents

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

System Requirements

Supported Hardware

Table 1 Supported Hardware

Device	Description	Supported by Minimum Cisco IOS Release
Catalyst 2360-48TD-S	48 10/100/1000 ports and four 10-Gigabit SFP+[1] module slots.	Cisco IOS Release 12.2(53)EY
Dual FRU Power Supplies		Cisco IOS Release 12.2(53)EY
SFP Modules	GE SFP, LC connector LX/LH transceiver GE SFP, LC connector SX transceiver	Cisco IOS Release 12.2(53)EY
SFP+ Modules	GBASE-LR SFP+ Module 10GBASE-SR SFP+ Module 10GBASE-LRM SFP+Module 10GBASE-LRM SFP+ Module for single mode 10GBASE-CX1 SFP+ Module	Cisco IOS Release 12.2(53)EY
C2360-PWR-135WAC	135-W AC-power-supply module	Cisco IOS Release 12.2(53)EY
C2360-FAN	60 CFM Fan Module	Cisco IOS Release 12.2(53)EY

1. SFP+ = 10 Gigabit fiber uplink.

Device Manager System Requirements

Hardware

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software

- Windows 2000, XP, Vista, and Windows Server 2003
- Internet Explorer 5.5, 6.0, 7.0, Firefox 1.5, 2.0

The device manager verifies the browser version when starting a session does not require a plug-in.

Cluster Compatibility

You cannot create and manage switch clusters through the device manager. Use the command-line interface (CLI).

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

- When you create a switch cluster, we recommend that you configure the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, configure 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 2360 switch, all standby command switches must be Catalyst 2360 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, and the command reference.

CNA Support

Cisco Network Assistant 5.4 and earlier does not provide specific device support for the Catalyst 2360 switch. For more information about Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

Upgrading the Switch Software

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.

Table 3 Cisco IOS Software Image Files

Filename	Description
Cisco Catalyst 2360-48TD-S	Catalyst 2360 image file and device manager files. This image has both Layer 2 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 from 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/prod/collateral/iosswrel/ps8802/ps6969/ps1835/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/prod_command_reference_list.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 new image file and replace or keep the current image.

Step 1 Use Table 3 on page 4 to identify the software image file that you want to download.

Step 2 Log in to the software download location:

http://www.cisco.com/cisco/web/download/index.html

a. Navigate to **Switches > LAN Switches - Access.**

b. Navigate to your switch model.

c. Click IOS Software, then select the latest IOS release.

d. Download the image you identified in Step 1.

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 a 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/c2360-univeresalk9-tar
```

This example shows how to download an image from a TFTP server and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option:

```
Switch# archive download-sw /leave-old-sw tftp://198.30.20.19/c2360-univeresalk9-tar
```

Recovering from a Software Failure

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

New Software Features

Table 4 Catalyst 2360 Switch Features

Feature	Minimum Cisco IOS Release Required
Online diagnostics to test the functionality of the supervisor engine, modules, and switch.	12.2(53)EY
On-board failure logging (OBFL) to collect information about the switch and any connected power supplies.	12.2(53)EY
SFP+ support for 10 Gigabit.	12.2(53)EY
USB mini-Type B console connection and RJ-45 console connection. Only one console connection can be active at a time.	12.2(53)EY
USB Type A port for access to external USB flash memory (thumb drives or USB keys).	12.2(53)EY

Configuration 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.

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.

Cisco IOS Limitations

None.

Important Notes

These sections describe the important notes related to this software release for the Catalyst 2360 switches:

Cisco IOS Notes

- 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, make sure that there is network connectivity between the switch and the ACS. You should also make sure that the switch has been properly configured as an AAA client on the ACS.

Device Manager Notes

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI.
- 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.

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** {**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 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

- CSCth20225

  Dynamic ARP inspection CLI is not functional.

  No workaround.

- CSCth27240

  Shaped Round Robin (SRR) commands are unavailable on the interface.

  No workaround.

Related Documentation

These documents provide complete information about the Catalyst 2360 switch and are available on Cisco.com:

http://www.cisco.com/en/US/products/ps10920/tsd_products_support_series_home.html

- *Catalyst 2360 Switch Getting Started Guide*
- *Catalyst 2360 Switch Hardware Installation Guide*
- *Catalyst 2360 Switch Command Reference*
- *Catalyst 2360 Switch Software Configuration Guide*
- *Catalyst 2360 Switch System Message Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 2360 Switches*
- *Product Documentation and Compliance for the Catalyst 2360 Switch*
- Device manager online help (available on the switch)

For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide.*

- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site:

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

  SFP 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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.