Release Notes for Catalyst 3750-E and Catalyst 3560-E Switches, Cisco IOS Release 12.2(46)SE

Revised October 20, 2011

Cisco IOS Release 12.2(46)SE and later runs on all Catalyst 3750-E and Catalyst 3560-E switches.

The Catalyst 3750-E switches support stacking through Cisco StackWise Plus technology. The Catalyst 3560-E switches do not support switch stacking. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 12.2(46)SE 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 6.
- 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 6.

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 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.

For the complete list of Catalyst 3750-E and Catalyst 3560-E switch documentation, see the "Related Documentation" section on page 32.

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 3750-E and Catalyst 3560-E Switches Supported Hardware

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
Cisco Catalyst 3750E-24TD	24 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3750E-48TD	48 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3750E-24PD	24 10/100/1000 PoE[1] ports, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3750E-48PD	48 10/100/1000 ports with 370 W of PoE, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2

Table 1 Catalyst 3750-E and Catalyst 3560-E Switches Supported Hardware (continued)

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
Cisco Catalyst 3750E-48PD Full Power	48 10/100/1000 ports with 740 W of PoE, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3560E-24TD	24 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3560E-48TD	48 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3560E-24PD	24 10/100/1000 PoE ports, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3560E-48PD	48 10/100/1000 ports with 370 W of PoE, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3560E-48PD Full Power	48 10/100/1000 ports with 740 W of PoE, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(35)SE2
Cisco Catalyst 3560E-12D	12 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(40)EX
Cisco Catalyst 3560E-12SD	12 SFP[2] module slots, 2 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(44)SE
Cisco X2 transceiver modules	X2-10GB-SR V02 or later X2-10GB-LR V03 or later X2-10GB-ER V02 or later X2-10GB-CX4 V03 or later X2-10GB-LX4 V03 or later X2-10GB-LRM	Cisco IOS Release 12.2(35)SE2 Cisco IOS Release 12.2(40)SE
Cisco TwinGig Converter Module	Dual SFP X2 converter module to allow the switch to support SFP Gigabit Ethernet modules	Cisco IOS Release 12.2(35)SE2
SFP modules	1000BASE-LX/LH 1000BASE-SX 1000BASE-ZX 1000BASE-BX10-D 1000BASE-BX10-U 1000BASE-T 100BASE-FX CWDM[3]	Cisco IOS Release 12.2(35)SE2
DOM[4] support for these SFP modules	X2-10GB-ER, X2-10GB-SR, X2-10GB-LR, X2-10GB-LRM GLC-ZX-SM, GLC-BX-D, GLC-BX-U SFP-GE-S, SFP-GE-L, SFP-GE-Z All CWDM and 32 DWDM SFP modules	Cisco IOS Release 12.2(46)SE

Table 1 Catalyst 3750-E and Catalyst 3560-E Switches Supported Hardware (continued)

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
SFP module patch cable[5]	CAB-SFP-50CM	Cisco IOS Release 12.2(35)SE2
C3K-PWR-1150WAC	1150-W AC power supply module for PoE-capable switches	Supported on all software releases
C3K-PWR-750WAC	750-W AC power supply module for PoE-capable switches	Supported on all software releases
C3K-PWR-265WAC	265-W AC power supply module for nonPoE-capable switches	Supported on all software releases
C3K-PWR-265WDC	265-W DC power supply module for nonPoE-capable switches	Supported on all software releases
C3K-BLWR-60CFM	Fan module	Supported on all software releases
Redundant power system (RPS)	Cisco RPS 2300 RPS	Supported on all software releases

1. PoE = Power over Ethernet.
2. SFP = small form-factor pluggable
3. CWDM = coarse wavelength-division multiplexer
4. DOM = digital optical monitoring
5. Only Catalyst 3560-E switches. The SFP module patch cable is a 0.5-meter, copper, passive cable with SFP module connectors at each end. The patch cable can connect two Catalyst 3560-E switches in a cascaded configuration.

Device Manager System Requirements

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

- "Hardware Requirements" section on page 4
- "Software Requirements" section on page 4

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
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB 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]	Netscape Navigator
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

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 3750-E switch, all standby command switches must be Catalyst 3750-E 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 Compatibility

Cisco IOS 12.2(35)SE2 and later is only compatible with Cisco Network Assistant 5.0 and later. You can download 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

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.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (IP base feature set or IP services feature set) and does not change if you upgrade the software license.

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 4 lists the filenames for this software release.

Note For IPv6 routing and IPv6 ACL capability on the Catalyst 3750-E or 3560-E switch, you must get the advanced IP services software license from Cisco.

Table 4 Cisco IOS Software Image Files

Filename	**Description**
c3750e-universal-tar.122-46.SE.tar	Catalyst 3750-E universal image and device manager files. This image has all the supported features that are enabled by the software license installed on the switch.
c3750e-universalk9-tar.122-46.SE.tar	Catalyst 3750-E universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, and SNMPv3 in addition to the features supported in the universal image.
c3560e-universal-tar.122-46.SE.tar	Catalyst 3560-E universal image and device manager files. This image has all the supported features that are enabled by the software license installed on the switch.
c3560e-universalk9-tar.122-46.SE.tar	Catalyst 3560-E universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, and SNMPv3 in addition to the features supported in the universal image.

The universal software images support multiple feature sets. Use the software activation feature to deploy a software license and to enable a specific feature set. For information about software activation, see the *Cisco Software Activation and Compatibility Document* on Cisco.com:

http://www.cisco.com/en/US/products/ps7077/tsd_products_support_series_home.html

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/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_book09186a00800811e0.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 Use Table 4 on page 7 to 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 universal software image files for a Catalyst 3750-E switch, click **Catalyst 3750-E software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3750-E 3DES Cryptographic Software**.

To download the universal software image files for a Catalyst 3560-E switch, click **Catalyst 3560-E software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3560-E 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/c3750e-universal-tar.122-46.SE.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

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

New Software Features

These are the new software features for this release:

- Generic message authentication support with the SSH Protocol and compliance with RFC 4256
- Voice aware IEEE 802.1x and mac authentication bypass (MAB) security violation to shut down only the data VLAN on a port when a security violation occurs
- Local web authentication banner so that custom banner or image file can be displayed at a web authentication login screen
- Support for the CISCO-NAC-NAD and CISCO-PAE MIBs
- Digital Optical Monitoring (DOM) of connected SFP modules
- The ability to exclude a port in a VLAN from the SVI line-state up or down calculation
- Support for HSRP Version 2 (HSRPv2)
- HSRP for IPv6 (requires the advanced IP services image)
- Disabling MAC address learning on a VLAN
- PAgP Interaction with Virtual Switches and Dual-Active Detection, also referred to as enhanced PAgP
- Support for rehosting a software license and for using an embedded evaluation software license
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down
- DHCP server port-based address allocation for the preassignment of an IP address to a switch port
- DHCP for IPv6 relay, client, server address assignment and prefix delegation (requires the advanced IP services image)
- IPv6 port-based trust with dual IPv4 and IPv6 SDM templates
- IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router

Minimum Cisco IOS Release for Major Features

Table 5 lists the minimum software release (after the first release) required to support the major features of the Catalyst 3750-E and Catalyst 3560-E switches. Features not listed are supported in all releases.

Table 5 Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Generic message authentication support with the SSH Protocol and compliance with RFC 4256	12.2(46)SE	3750-E, 3560-E
Voice aware IEEE 802.1x and mac authentication bypass (MAB) security violation	12.2(46)SE	3750-E, 3560-E
Local web authentication banner	12.2(46)SE	3750-E, 3560-E
Support for the CISCO-NAC-NAD and CISCO-PAE MIBs	12.2(46)SE	3750-E, 3560-E
Digital Optical Monitoring (DOM) of connected SFP modules	12.2(46)SE	3750-E, 3560-E
The ability to exclude a port in a VLAN from the SVI line-state up or down calculation	12.2(46)SE	3750-E, 3560-E
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE	3750-E, 3560-E
HSRP for IPv6 (requires the advanced IP services image)	12.2(46)SE	3750-E, 3560-E
Disabling MAC address learning on a VLAN	12.2(46)SE	3750-E, 3560-E
PAgP Interaction with Virtual Switches and Dual-Active Detection	12.2(46)SE	3750-E, 3560-E
Support for rehosting a software license and for using an embedded evaluation software license	12.2(46)SE	3750-E, 3560-E
EOT and IP SLAs EOT static route support	12.2(46)SE	3750-E, 3560-E
DHCP server port-based address allocation	12.2(46)SE	3750-E, 3560-E
DHCP for IPv6 relay, client, server address assignment and prefix delegation (requires the advanced IP services image	12.2(46)SE	3750-E, 3560-E
IPv6 port-based trust with dual IPv4 and IPv6 SDM templates	12.2(46)SE	3750-E, 3560-E
IPv6 default router preference (DRP)	12.2(46)SE	3750-E, 3560-E
Embedded event manager (EEM) for device and system management (IP service image only)	12.2(46)SE	3750-E, 3560-E
DHCP-based autoconfiguration and image update	12.2(44)SE	3750-E, 3560-E
Configurable small-frame arrival threshold	12.2(44)SE	3750-E, 3560-E
Digital optical monitoring (DOM)	12.2(44)SE	3750-E, 3560-E
Source Specific Multicast (SSM) mapping	12.2(44)SE	3750-E, 3560-E
HTTP and HTTP(s) support over IPV6	12.2(44)SE	3750-E, 3560-E
Simple Network and Management Protocol (SNMP) configuration over IPv6 transport	12.2(44)SE	3750-E, 3560-E
IPv6 support for stateless autoconfiguration	12.2(44)SE	3750-E, 3560-E
Flex Link Multicast Fast Convergence	12.2(44)SE	3750-E, 3560-E
IEEE 802.1x readiness check	12.2(44)SE	3750-E, 3560-E

Table 5 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
/31 bit mask support for multicast traffic	12.2(44)SE	3750-E, 3560-E
Flow-based Switch Port Analyzer (FSPAN)	12.2(44)SE	3750-E, 3560-E
Automatic quality of service (QoS) Voice over IP (VoIP) enhancement	12.2(40)SE	3750-E, 3560-E
Configuration replacement and rollback	12.2(40)SE	3750-E, 3560-E
Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)	12.2(40)SE	3750-E, 3560-E
Internet Group Management Protocol (IGMP) Helper	12.2(40)SE	3750-E, 3560-E
IP Service Level Agreements (IP SLAs)	12.2(40)SE	3750-E, 3560-E
IP SLAs EOT	12.2(40)SE	3750-E, 3560-E
Multicast virtual routing and forwarding (VRF) Lite	12.2(40)SE	3750-E, 3560-E
SSM PIM protocol	12.2(40)SE	3750-E, 3560-E
Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6	12.2(40)SE	3750-E, 3560-E
Support for VRF-aware services	12.2(40)SE	3750-E, 3560-E
Support for the Link Layer Discovery Protocol Media Extensions (LLDP-MED) location TLV	12.2(40)SE	3750-E, 3560-E
Support for the CISCO-MAC-NOTIFICATION-MIB	12.2(40)SE	3750-E, 3560-E
Support for the CISCO-POWER-ETHERNET-EXT-MIB	12.2(40)SE	3750-E, 3560-E
DHCP Snooping Statistics **show** and **clear** commands	12.2(37)SE	3750-E, 3560-E
IP phone detection enhancement	12.2(37)SE	3750-E, 3560-E
IP unicast reverse path forwarding (unicast RPF)	12.2(37)SE	3750-E, 3560-E
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(37)SE	3750-E, 3560-E
PIM stub routing in the IP base image	12.2(37)SE	3750-E, 3560-E
Port security on a PVLAN host	12.2(37)SE	3750-E, 3560-E
VLAN aware port security option	12.2(37)SE	3750-E, 3560-E
Support for auto-rendezvous point (auto-RP) for IP multicast	12.2(37)SE	3750-E, 3560-E
VLAN Flex Link Load Balancing	12.2(37)SE	3750-E, 3560-E
Web Cache Communication Protocol (WCCP)	12.2(37)SE	3750-E, 3560-E
SNMP support for the Port Error Disable MIB	12.2(37)SE	3750-E, 3560-E
Support for the Time Domain Reflectometry MIB	12.2(37)SE	3750-E, 3560-E

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

Unless otherwise noted, these limitations apply to the Catalyst 3750-E and 3560-E switches:

Access Control List

These are the access control list (ACL) limitations:

- The Catalyst 3750-E and Catalyst 3560-E switches have 964 TCAM entries available for ACLs in the default and routing SDM templates instead of the 1024 entries that are available on the Catalyst 3560 and Catalyst 3750 switches.

  There is no workaround. (CSCse33114)

- When a MAC access list is used to block packets from a specific source MAC address, that MAC address is entered in the switch MAC-address table.

  The workaround is to block traffic from the specific MAC address by using the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command. (CSCse73823)

Address Resolution Protocol

This is an Address Resolution Protocol limitation:

- 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.(CSCse06827))

Cisco Redundant Power System 2300

This is the Cisco Redundant Power System (RPS) 2300 limitation:

- When connecting the RPS cable between the RPS 2300 and the Catalyst 3750-E or 3560-E switch or other supported network devices, this communication error might appear:

  ```
  PLATFORM_ENV-1-RPS_ACCESS: RPS is not responding
  ```

  No workaround is required because the problem corrects itself. (CSCsf15170)

Cisco X2 Transceiver Modules and SFP Modules

These are the Cisco X2 transceiver module and SFP module limitations:

- Cisco X2-10GB-CX4 transceiver modules with a version identification number lower than V03 might be difficult to insert because of a dimensional tolerance discrepancy. The workaround is to use modules with a version identification number of V03 or later. (CSCsg28558)
- Switches with the Cisco X2-10GB-LX4 transceiver modules with a version identification number prior to V03 might intermittently fail. The workaround is to use Cisco X2-10GB-LX4 transceiver modules with a version identification number of V03 or later. (CSCsh60076)
- Cisco GLC-GE-100FX SFP modules with a serial number between OPC0926xxxx and OPC0945xxxx might show intermittent *module not valid*, data, status, link-flapping, and FCS errors. The workaround is to use modules with serial numbers that are not in the specified range. (CSCsh59585)
- When switches are installed closely together and the uplink ports of adjacent switches are in use, you might have problems accessing the SFP module bale-clasp latch to remove the SFP module or the SFP cable (Ethernet or fiber). Use one of these workarounds:
  - Allow space between the switches when installing them.
  - In a switch stack, plan the SFP module and cable installation so that uplinks in adjacent stack members are not all in use.
  - Use long, small screwdriver to access the latch then remove the SFP module and cable. (CSCsd57938)
- When a Cisco X2-10GB-CX4 transceiver module is in the X2 transceiver module port and you enter the **show controllers ethernet-controller tengigabitethernet** privileged EXEC command, the command displays some fields as unspecified. This is the expected behavior based IEEE 802.3ae. (CSCsd47344)
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module. The workaround is to configure aggressive UDLD. (CSCsh70244).

Configuration

These are the configuration limitations:

- When an excessive number (more than 100 packets per second) of Address Resolution Protocol (ARP) packets are sent to a Network Admission Control (NAC) Layer 2 IP-configured member port, a switch might display a message similar to this:

  ```
  PLATFORM_RPC-3-MSG_THROTTLED: RPC Msg Dropped by throttle mechanism: type 0, class
  51, max_msg 128, total throttled 984323

  -Traceback= 6625EC 5DB4C0 5DAA98 55CA80 A2F2E0 A268D8
  ```

  No workaround is necessary. Under normal conditions, the switch generates this notification when snooping the next ARP packet. (CSCse47548)

- When there is a VLAN with protected ports configured in fallback bridge group, packets might not be forwarded between the protected ports.

  The workaround is to not configure VLANs with protected ports as part of a fallback bridge group. (CSCsg40322)

  When a switch port configuration is set at 10 Mb/s half duplex, sometimes the port does not send in one direction until the port traffic is stopped and then restarted. You can detect the condition by using the **show controller ethernet-controller** or the **show interfaces** privileged EXEC commands.

  The workaround is to stop the traffic in the direction in which it is not being forwarded, and then restart it after 2 seconds. You can also use the **shutdown** interface configuration command followed by the **no shutdown** command on the interface. (CSCsh04301)

- 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.(CSCsi26392)

EtherChannel

These are the EtherChannel limitations:

- In an EtherChannel running Link Aggregation Control Protocol (LACP), the ports might be put in the suspended or error-disabled state after a stack partitions or a member switch reloads. This occurs when:
  - The EtherChannel is a cross-stack EtherChannel with a switch stack at one or both ends.
  - The switch stack partitions because a member reloads. The EtherChannel is divided between the two partitioned stacks, each with a stack master.

  The EtherChannel ports are put in the suspended state because each partitioned stack sends LACP packets with different LACP Link Aggregation IDs (the system IDs are different). The ports that receive the packets detect the incompatibility and shut down some of the ports. Use one of these workarounds for ports in this error-disabled state:
  - Enable the switch to recover from the error-disabled state.
  - Enter the **shutdown** and the **no shutdown** interface configuration commands to enable the port.

  The EtherChannel ports are put in the error-disabled state because the switches in the partitioned stacks send STP BPDUs. The switch or stack at the other end of the EtherChannel receiving the multiple BPDUs with different source MAC addresses detects an EtherChannel misconfiguration.

After the partitioned stacks merge, ports in the suspended state should automatically recover. (CSCse33842)

- When a switch stack is configured with a cross-stack EtherChannel, it might transmit duplicate packets across the EtherChannel when a physical port in the EtherChannel has a link-up or link-down event. This can occur for a few milliseconds while the switch stack adjusts the EtherChannel for the new set of active physical ports and can happen when the cross-stack EtherChannel is configured with either mode ON or LACP. This problem might not occur with all link-up or link-down events.

  No workaround is necessary. The problem corrects itself after the link-up or link-down event. (CSCse75508)

- The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:

  ```
  15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
  (ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
  4CEB50 859DF4 A7BF28 A98260 882658 879A58
  ```

  There is no workaround. (CSCsh12472)

IEEE 802.1x Authentication

These are the IEEE 802.1x authentication limitations:

- If a supplicant using a Marvel Yukon network interface card (NIC) is connected an IEEE 802.1x-authorized port in multihost mode, the extra MAC address of 0c00.0000.0000 appears in the MAC address table.

  Use one of these workarounds (CSCsd90495):

  - Configure the port for single-host mode to prevent the extra MAC address from appearing in the MAC address table.
  - Replace the NIC card with a new card.

- When MAC authentication bypass is configured to use Extensible Authentication Protocol (EAP) for authorization and critical authentication is configured to assign a critical port to an access VLAN:

  - If the connected device is supposed to be unauthorized, the connected device might be authorized on the VLAN that is assigned to the critical port instead of to a guest VLAN.
  - If the device is supposed to be authorized, it is authorized on the VLAN that is assigned to the critical port.

  Use one of these workarounds (CSCse04534):

  - Configure MAC authentication bypass to not use EAP.
  - Define your network access profiles to not use MAC authentication bypass. For more information, see the Cisco Access Control Server (ACS) documentation.

- When IEEE 802.1x authentication with VLAN assignment is enabled, a CPUHOG message might appear if the switch is authenticating supplicants in a switch stack.

  The workaround is not use the VLAN assignment option. (CSCse22791)

Multicasting

These are the multicasting limitations:

- Multicast packets with a time-to-live (TTL) value of 0 or 1 are flooded in the incoming VLAN when all of these conditions are met:
  - Multicast routing is enabled in the VLAN.
  - The source IP address of the packet belongs to the directly connected network.
  - The TTL value is either 0 or 1.

  The workaround is to not generate multicast packets with a TTL value of 0 or 1, or disable multicast routing in the VLAN. (CSCeh21660)
- Multicast packets denied by the multicast boundary access list are flooded in the incoming VLAN when all of these conditions are met:
  - Multicast routing is enabled in the VLAN.
  - The source IP address of the multicast packet belongs to a directly connected network.
  - The packet is denied by the IP multicast boundary access-list configured on the VLAN.

  There is no workaround. (CSCei08359)
- Reverse path forwarding (RPF) failed multicast traffic might cause a flood of Protocol Independent Multicast (PIM) messages in the VLAN when a packet source IP address is not reachable.

  The workaround is to not send RPF-failed multicast traffic, or make sure that the source IP address of the RPF-failed packet is reachable. (CSCsd28944)
- If the **clear ip mroute** privileged EXEC command is used when multicast packets are present, it might cause temporary flooding of incoming multicast traffic in the VLAN.

  There is no workaround. (CSCsd45753)
- When you configure the **ip igmp max-groups** *number* and **ip igmp max-groups action replace** interface configuration commands and the number of reports exceed the configured max-groups value, the number of groups might temporarily exceed the configured max-groups value. No workaround is necessary because the problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)
- When you configure the IGMP snooping throttle limit by using the **ip igmp max-groups** *number* interface configuration on a port-channel interface, the groups learned on the port-channel might exceed the configured throttle limit number, when all of these conditions are true:
  - The port-channel is configured with member ports across different switches in the stack.
  - When one of the member switches reloads.
  - The member switch that is reloading has a high rate of IP IGMP joins arriving on the port-channel member port.

  The workaround is to disable the IGMP snooping throttle limit by using the **no ip igmp max-groups** *number* interface configuration command and then to reconfigure the same limit again. (CSCse39909)

PoE

These are the power-over-Ethernet (PoE) limitations:

- When a loopback cable is connected to a switch PoE port, the **show interface status** privileged EXEC command shows *not connected*, and the link remains down. When the same loopback cable is connected to a non-PoE port, the link becomes active and then transitions to the error-disabled state when the **keepalive** feature is enabled. There is no workaround. (CSCsd60647)
- The Cisco 7905 IP Phone is error-disabled when the phone is connected to an external power source.

  The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)
- The pethPsePortShortCounter MIB object appears as *short* even though the powered device is powered on after it is connected to the PoE port.

  There is no workaround. (CSCsg20629)

QoS

These are the quality of service (QoS) limitations:

- When QoS is enabled and the egress port receives pause frames at the line rate, the port cannot send packets.

  There is no workaround. (CSCeh18677)
- Egress shaped round robin (SRR) sharing weights do not work properly with system jumbo MTU frames.

  There is no workaround. (CSCsc63334)
- In a hierarchical policy map, if the VLAN-level policy map is attached to a VLAN interface and the name of the interface-level policy map is the same as that for another VLAN-level policy map, the switch rejects the configuration, and the VLAN-level policy map is removed from the interface.

  The workaround is to use a different name for the interface-level policy map. (CSCsd84001)
- If the ingress queue has low buffer settings and the switch sends multiple data streams of system jumbo MTU frames at the same time at the line rate, the frames are dropped at the ingress.

  There is no workaround. (CSCsd72001)
- When you use the **srr-queue bandwidth limit** interface configuration command to limit port bandwidth, packets that are less than 256 bytes can cause inaccurate port bandwidth readings. The accuracy is improved when the packet size is greater than 512 bytes. There is no workaround. (CSCsg79627)

Routing

These are the routing limitations:

- The switch stack might reload if the switch runs with this configuration for several hours, depleting the switch memory and causing the switch to fail:
  - The switch has 400 Open Shortest Path First (OSPF) neighbors.
  - The switch has thousands of OSPF routes.

  The workaround is to reduce the number of OSPF neighbors to 200 or less. (CSCse65252)

- When the PBR is enabled and QoS is enabled with DSCP settings, the CPU utilization might be high if traffic is sent to unknown destinations.

  The workaround is to not send traffic to unknown destinations. (CSCse97660)

SPAN and RSPAN

This is the SPAN and Remote SPAN (RSPAN) limitation.

- When egress SPAN is running on a 10-Gigabit Ethernet port, only about 12 percent of the egress traffic is monitored.

  There is no workaround. This is a hardware limitation. (CSCei10129)

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).

VLANs

These are the VLAN limitations:

- When the domain is authorized in the guest VLAN on a member switch port without link loss and an Extensible Authentication Protocol over LAN (EAPOL) is sent to an IEEE 802.1x supplicant to authenticate, the authentication fails. This problem happens intermittently with certain stacking configurations and only occurs on the member switches.

  The workaround is to enter the **shut** and **no shut** interface configuration commands on the port to reset the authentication status. (CSCsf98557)

- 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. (CSCsi26444)

Stacking (only Catalyst 3750-E Switch Stack)

These are the Catalyst 3750-E switch stack limitations:

- Where there is a mixed hardware stack with Catalyst 3750-E and 3750 switches as stack members, when you change the configuration and enter the **write memory** privileged EXEC command, the `unable to read config` message appears.

  The workaround is to wait a few seconds and then to reenter the **write memory** privileged EXEC command. (CSCsd66272)

- When using the **logging console** global configuration command, low-level messages appear on both the stack master and the stack member consoles.

  The workaround is to use the **logging monitor** global configuration command to set the severity level to block the low-level messages on the stack member consoles. (CSCsd79037)

- In a mixed stack which consists of Catalyst 3750 switches along with Catalyst 3750-E switches, when the stack ring is congested with approximately 40 Gb/s of traffic, some of the local traffic from one port to another on a Catalyst 3750-E member might be dropped.

  The workaround is to avoid traffic congestion on the stack ring. (CSCsd87538)

- If a new member switch joins a switch stack within 30 seconds of a command to copy the switch configuration to the running configuration of the stack master, the new member might not get the latest running configuration and might not operate properly.

  The workaround is to reboot the new member switch. Use the **remote command all show run** privileged EXEC command to compare the running configurations of the stack members. (CSCsf31301)

- When the flash memory of a stack member is almost full, it might take longer to start up than other member switches. This might cause that switch to miss the stack-master election window. As a result, the switch might fail to become the stack master even though it has the highest priority.

  The workaround is to delete files in the flash memory to create more free space. (CSCsg30073)

- In a mixed stack of Catalyst 3750 switches and Catalyst 3750-E switches, when the stack reloads, the Catalyst 3750-E might not become stack master, even it has a higher switch priority set.

  The workaround is to check the flash. If it contains many files, remove the unnecessary ones. Check the lost and found directory in flash and if there are many files, delete them. To check the number of files use the **fsck flash:** command. (CSCsi69447)

- After a stack bootup, the spanning tree state of a port that has IEEE 802.1x enabled might be blocked, even when the port is in the authenticated state. This can occur on a voice port where the Port Fast feature is enabled.

  The workaround is to enter a **shutdown** interface configuration command followed by a **no shutdown** command on the port in the blocked state. (CSCsl64124)

Device Manager Limitations

This is the device manager limitation:

- 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 3750-E and 3560-E switches:

- "Switch Stack Notes" section on page 21
- "Cisco IOS Notes" section on page 21
- "Device Manager Notes" section on page 21

Switch Stack Notes

These notes apply to switch stacks:

- Always power off a switch before adding or removing it from a switch stack.
- The Catalyst 3560-E switches do not support switch stacking. However, the **show processes** privileged EXEC command still lists stack-related processes. This occurs because these switches share common code with other switches that do support stacking.
- Catalyst 3750-E switches running Cisco IOS Release 12.2(35)SE2 are compatible with Catalyst 3750 switches and Cisco EtherSwitch service modules running Cisco IOS Release 12.2(35)SE. Catalyst 3750-E switches, Catalyst 3750 switches, and Cisco EtherSwitch service modules can be in the same switch stack. In this switch stack, we recommend that the Catalyst 3750-E switch be the stack master.

Cisco IOS Notes

These notes apply 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, 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.
- If the switch has interfaces with automatic QoS for voice over IP (VoIP) configured and you upgrade the switch software to Cisco IOS Release 12.2(40)SE (or later), when you enter the **auto qos voip cisco-phone** interface configuration command on another interface, you might see this message:

  ```
  AutoQoS Error: ciscophone input service policy was not properly applied
  policy map AutoQoS-Police-CiscoPhone not configured
  ```

  If this happens, enter the **no auto qos voip cisco-phone** interface command on all interface with this configuration to delete it. Then enter the **auto qos voip cisco-phone** command on each of these interfaces to reapply the configuration.

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 with possible unexpected activity in this software release. Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the Catalyst 3750-E and 3560-E switches:

- CSCsk65142

  When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command.

- CSCsk96058 (Catalyst 3750-E switches)

  A stack member switch might fail to bundle Layer 2 protocol tunnel ports into a port channel when you have followed these steps:

  1. You configure a Layer 2 protocol tunnel port on the master switch.
  2. You configure a Layer 2 protocol tunnel port on the member switch.
  3. You add the port channel to the Layer 2 protocol tunnel port on the master switch.
  4. You add the port channel to the Layer 2 protocol tunnel port on the member switch.

  After this sequence of steps, the member port might stay suspended.

  The workaround is to configure the port on the member switch as a Layer 2 protocol tunnel and at the same time also as a port channel. For example:

```
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# channel-group 1 mode on
```

- CSCsl02680

  When the configuration file is removed from the switch and the switch is rebooted, port status for VLAN 1 and the management port (Fast Ethernet 0) is sometimes reported as `up` and sometimes as `down`, resulting in conflicts. This status depends on when you respond to the reboot query:

  ```
  Would you like to enter the initial configuration dialog?
  ```

  - After a reboot if you wait until the Line Protocol status of VLAN 1 appears on the console before responding, VLAN 1 line status is always shown as `down`. This is the correct state.
  - The problem (VLAN 1 reporting `up`) occurs if you respond to the query before VLAN 1 line status appears on the console.

  The workaround is to wait for approximately 1 minute after rebooting and until the VLAN 1 interface line status appears on the console before you respond to the query.

- CSCso96778

  When you use the **ipv6 address dhcp** interface configuration command on an interface that is configured in router mode, other addresses on the prefix associated with the new address might not be accessible.

  The workaround is to use the **ipv6 address dhcp** interface configuration command on an interface that is configured in host mode, or configure a static route to the prefix through the interface.

- CSCsr65689 (Catalyst 3750-E switches)

  When loopback interfaces are configured, this error message might appear when a stack member is loading:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2
  ```

  No workaround is required. This does not affect switch functionality.

Resolved Caveats

These are the caveats that have been resolved in this release. Unless otherwise noted, these resolved caveats apply to both the Catalyst 3750-E and 3560-E switches.

- CSCin91851, CSCsh42013, and CSCsh42316

  The SSH Protocol now supports generic message authentication and is compliant with RFC 4256.

- CSCsa73179

  A switch no longer fails under these conditions:

  - `OSPF is in the switch image`.
  - You enter the RIP **no default-information** router configuration command.

- CSCse07265

  If you configure IP SLA to generate a syslog message for a reaction trap and an operation with a trigger of *timeout* or *connectionless,* a syslog message now appears when triggered.

- CSCsi70454

  The configuration file used for the configuration replacement feature no longer requires the character string *end\n* at the end of the file.

- CSCsi71768

  If you upgrade the software image from Cisco IOS Release 12.2(25)SEE2 to Cisco IOS Release 12.2(35)SE1, the IPv6 static routes are now saved in the routing table.

- CSCsj10198

  When a per-port per-VLAN policy map (a hierarchical VLAN-based policy map) is attached to a VLAN interface and you remove the child-policy policer from the policy map and then restore it, the policy map now correctly re-attaches to the same SVI.

- CSCsk09459

  When a switch stack boots up, traceback messages no longer appear on the console when the switch stack has 400 or more VLANs and multicast or port-security features.

- CSCsk47893

  A switch running the IP base image now supports full EIGRP stub routing.

- CSCsl72968 (Catalyst 3750-E switches)

  When multidomain authentication (MDA) is configured on a stack member, a switch port in that stack is no longer intermittently enter disabled when the stack reloads.

- CSCsl19426 (Catalyst 3560-E switches)

  Inserting or removing a power-supply module in a Catalyst 3560E-12D or 3560E-12SD switch enabled with SNMP now generates a trap.

- CSCso22855

  If you specify the router ID before entering the **autonomous-system** *autonomous-system-number* address-family configuration command, the router ID is no longer lost when the switch reloads.

- CSCso22883

  Any form of the **passive-interface** command entered in one instance propagates to all configured address-family instances for the same EIGRP routing process.

- CSCso40282 (Catalyst 3750-E switches)

  A switch stack no longer stops sending CDP packets when more than 100 IP phones are connected to the stack.

- CSCso70893 (Catalyst 3750-E switches)

  A message similar to this one no longer appears when you log into a switch through an SSH session and upgrade the switch by using the **archive download-sw** privileged EXEC command

  ```
  *Mar 11 06:48:22.729 JST: %SCHED-3-THRASHING: Process thrashing on watched message
  event. -Process= "SSH Process", ipl= 6, pid= 147
  ```

- CSCso72052

  An end host no longer remains in the guest VLAN after IEEE 802.1X authentication.

- CSCso81660 (Catalyst 3750-E switches)

  The **show interfaces** command output for a switch stack now shows the correct values for the output drops.

- CSCso92369

  A switch no longer unexpectedly reloads when the **show license status** privileged EXEC command is entered multiple times

  A switch may unexpectedly reload. In previous releases, the switch crash file indicates these reloads were caused by memory corruptions.

- CSCsq17094 (Catalyst 3750-E switches)

  Downstream switch interfaces in a link state group no longer fail under these conditions:

  - The switch is part of a stack.
  - There is a master switch over.
  - Some (or all) of the link state group interfaces are on the switch that becomes the new stack master.

- CSCsq27267 (Catalyst 3750-E switches)

  A switch stack now sends VTP join message for a VLAN interface without access ports associated with it.

- CSCsq38082

  The cluster configuration is now saved to each cluster member when you save the configuration to the cluster commander.

- CSCsr50978 (Catalyst 3750-E switches)

  An EtherChannel with ports across stack members and configured to tunnel Layer 2 protocol packets (using the **l2protocol-tunnel** interface configuration command), no longer drops protocol packets received on a switch in the EtherChannel that is not the stack master.

- CSCsr55949

  When IEEE 802.1x is enabled on the switch, EAP notification packets are no longer dropped.

Documentation Updates

These sections provide updates to the product documentation:

- "Updates to the Software Configuration Guide" section on page 26
- "Updates to the System Message Guide" section on page 27
- "Updates to the Getting Started Guides" section on page 32

Updates to the Software Configuration Guide

- In the "Configuration Guidelines" section of the "Configuring Flex Links and the MAC Address-Table Move Update Feature" chapter, this guideline is added:

  You can configure up to 16 backup links.

- This information is added to the "Using Route Maps to Redistribute Routing Information" section in the "Configuring IP Unicast Routing" chapter:

Note A route map with no **set** route-map configuration commands is sent to the CPU, which causes high CPU utilization.

- Unsupported Embedded Event Manager Commands

  Privileged EXEC

  event manager scheduler clear

  event manager update user policy

show event manager detector

show event manager version

Global Configuration

event manager detector rpc

event manager directory user repository

Applet Configuration (config-applet)

event rpc

event snmp-notification

trigger (EEM)

Trigger Applet Configuration (config-applet-trigger)

attribute (EEM)

correlate

Event Trigger Configuration (config-event-trigger)

event owner

Updates to the System Message Guide

This section contains the system message guide updates.

New System Messages

These messages were added to the system message guide:

Error Message `ACLMGR-4-UNLOADINGFSPAN Unloading[chars]session[dec][chars]feature`

Explanation The access control list (ACL) manager is unable to store the flow-based SPAN (FSPAN) configuration, and this feature has been temporarily disabled for the specified session. The first [chars] is the type of FSPAN session: either *vlan-based FSPAN* for a VLAN FSPAN session or *port-based FSPAN* for a port FSPAN session. [dec] is the session number, and the second [chars] is the type of traffic being filtered: *MAC, IPv4, or IPv6*.

Recommended Action Specify an SDM template that allocates more system resources for ACLs, simplify the ACL, or use the same ACLs on multiple interfaces.

Error Message `ACLMGR-4-RELOADEDFSPAN Reloading [chars] session [dec] [chars] feature`

Explanation The access control list (ACL) manager can store the flow-based SPAN configuration for the specified session. One or more ACLs had previously been unloaded because of lack of hardware memory. The first [chars] is the type of FSPAN session: either *vlan-based FSPAN* for a VLAN FSPAN session or *port-based FSPAN* for a port FSPAN session. [dec] is the session number, and the second [chars] is the type of traffic being filtered: *MAC, IPv4, or IPv6*.

Recommended Action No action is required.

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars]`

Explanation The client MAC address could not be added to the MAC address table because the hardware memory is full or the address is a secure address on another port. [enet] is the supplicant MAC address, and [chars] is the interface. This message might appear if the IEEE 802.1x feature is enabled.

Recommended Action If the hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, manually remove it from that port.

Error Message `EC-5-CANNOT_BUNDLE1: Port-channel [chars] is down, port [chars] will remain stand-alone.`

Explanation The aggregation port is down. The port remains standalone until the aggregation port is up. The first [chars] is the EtherChannel. The second [chars] is the port number.

Recommended Action Ensure that the other ports in the bundle have the same configuration]

Error Message `ILPOWER-3-CONTROLLER_PORT_ERR:Controller port error, Interface Fa0/7:Power given, but link is not up.`

Explanation The inline-power-controller reported an error on an interface.

Recommended Action Enter the **shutdown** and **no shutdown** interface configuration commands on the affected interfaces. Upgrade to Cisco IOS Release12.1(14)EA1 or later, which provides an electrostatic discharge (ESD) recovery mechanism.

Error Message `%PAGP_DUAL_ACTIVE-3-OBJECT_CREATE_FAILED: Unable to create [chars]`

Explanation The switch cannot create the specified managed object. [chars] is the object name.

Recommended Action No action is required.

Error Message `%PAGP_DUAL_ACTIVE-3-RECOVERY_TRIGGER: PAgP running on [chars] informing virtual switches of dual-active: new active id [enet], old id [enet]`

Explanation Port Aggregation Protocol (PAgP) received a new active ID on the specified interface, which means that all virtual switches are in a dual-active scenario. The interface is informing virtual switches of this, which causes one switch to go into recovery mode. [chars] is the interface. The first [enet] is the new active ID. The second [enet] is the ID that it replaces.

Recommended Action No action is required.

Error Message `%PAGP_DUAL_ACTIVE-3-REGISTRY_ADD_ERR: Failure in adding to [chars] registry`

Explanation The switch could not add a function to the registry. [chars] is the registry name.

Recommended Action No action is required.

Error Message `PLATFORM_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix`

Explanation A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ip unicast failed route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

Error Message `PLATFORM_HCEF-3-ADJ: [chars]`

Explanation This message appears when an unsupported feature is configured on a switch running Cisco IOS Release 12.2(25)SE. [chars] is the error message.

Recommended Action Determine if a generic routing encapsulation (GRE) tunnel or the **ip cef accounting** global configuration command are configured. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnels are supported. If the GRE tunnel is configured, remove the tunnel, or upgrade the switch software to a Cisco IOS release when the GRE feature is needed. If the **ip cef accounting** command is configured, remove it by using the **no ip cef accounting** global configuration command.

Note Cisco IOS Release12.2(25)SEB2 does not support the **ip cef accounting** command.

Error Message `PLATFORM_IPv6_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix`

Explanation A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ipv6 unicast retry route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

Error Message `PLATFORM_SPAN-3-FEATUREMISMATCH:[chars] cannot be supported with the image running on switch [dec].`

Explanation A switch stack member software image does not support a specific flow-based SPAN (FSPAN) access control list (ACL) filter. [chars] is the FSPAN ACL filter that is not supported, and [dec] is the stack member number.

Recommended Action Upgrade to an image that supports the FSPAN ACL filter.

Error Message `%PM-6-EXT_VLAN_ADDITION: Extended VLAN is not allowed to be configured in VTP CLIENT mode.`

Explanation The switch did not add a VLAN in VTP client mode.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section in the system message guides.

Error Message `SPANTREE-6-PORTADD_ALL_VLANS: [chars] added to all Vlans`

Explanation The interface has been added to all VLANs. [chars] is the added interface.

Recommended Action No action is required.

Error Message `SPANTREE-6-PORTDEL_ALL_VLANS: [chars] deleted from all Vlans`

Explanation The interface has been deleted from all VLANs. [chars] is the deleted interface.

Recommended Action No action is required.

Error Message `SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to [chars].`

Explanation The VLAN Trunking Protocol (VTP) domain name was changed through the configuration to the name specified in the message. [chars] is the changed domain name.

Recommended Action No action is required.

Error Message `VQPCLIENT-2-TOOMANY: Interface [chars] shutdown by active host limit.`

Explanation The system has shut down the specified interface because too many hosts have requested access to that interface. [chars] is the interface name.

Recommended Action To enable the interface, remove the excess hosts, and enter the **no shutdown** interface configuration command.

Error Message `VQPCLIENT-3-VLANNAME: Invalid VLAN [chars] in response.`

Explanation The VLAN membership policy server (VMPS) has specified a VLAN name that is unknown to the switch. [chars] is the VLAN name.

Recommended Action Ensure that the VLAN exists on the switch. Verify the VMPS configuration by entering the **show vmps** privileged EXEC command.

Error Message `WCCP-5-CACHEFOUND: Web Cache [IP_address] acquired.`

Explanation The switch has acquired the specified web cache. [IP_address] is the web cache IP address.

Recommended Action No action is required.

Error Message `WCCP-1-CACHELOST: Web Cache [IP_address] lost.`

Explanation The switch has lost contact with the specified web cache. [IP_address] is the web cache IP address.

Recommended Action Verify the operation of the web cache by entering the **show ip wccp web-cache** privileged EXEC command.

Deleted System Messages

These messages were deleted from the system message guide:

Error Message `%VQPCLIENT-2-INITFAIL: Platform-specific VQP initialization failed. Quitting`

Error Message `%VQPCLIENT-2-IPSOCK: Could not obtain IP socket`

Error Message `%VQPCLIENT-7-NEXTSERV: Trying next VMPS [IP_address]`

Error Message `%VQPCLIENT-7-PROBE: Probing primary server [IP_address]`

Error Message `%VQPCLIENT-2-PROCFAIL: Could not create process for VQP. Quitting`

Error Message `%VQPCLIENT-7-RECONF: Reconfirming VMPS responses`

Error Message `%VQPCLIENT-2-SHUTDOWN: Interface [chars] shutdown by VMPS`

Error Message `%VQPCLIENT-3-THROTTLE: Throttling VLAN change on [chars]`

Updates to the Getting Started Guides

These are the updates to the Getting Started Guides for the Catalyst 3750-E and Catalyst 3560-E switches:

- This information should be included in the "Install and Connect to Devices in the 10-Gigabit Ethernet Slots" section:
  - When you install or remove the converter module, the mode on the switch changes from 10-Gigabit Ethernet to Gigabit Ethernet or the reverse. During this mode change, data traffic on the other switch uplink ports (X2 transceiver or SFP module ports) might temporarily stop.
  - When you install or remove an X2 transceiver or SFP module, traffic delay does not occur.
- This information should be included in the "Troubleshooting Express Setup" section:
  - POST errors are usually fatal. Contact your Cisco technical support representative if your switch fails POST.

Related Documentation

These documents provide complete information about the Catalyst 3750-E and Catalyst 3560-E switches and are available on Cisco.com:

http://www.cisco.com/en/US/products/ps7077/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/ps7078/tsd_products_support_series_home.html

These documents provide complete information about the switches:

- Catalyst 3750-E Switch Getting Started Guide
- Catalyst 3560-E Switch Getting Started Guide
- *Catalyst 3750-E and Catalyst 3560-E Switch Hardware Installation Guide*
- Regulatory Compliance and Safety Information for the Catalyst 3750-E and *Catalyst* 3560-E Switch
- *Release Notes for the Catalyst 3750-E and Catalyst 3560-E Switch*
- *Catalyst 3750-E and Catalyst 3560-E Switch Software Configuration Guide*
- *Catalyst 3750-E and Catalyst 3560-E Switch Command Reference*
- *Catalyst 3750-E and Catalyst 3560-E Switch System Message Guide*
- *Cisco Software Activation and Compatibility Document*
- *Installation Notes for the Catalyst 3750-E, Catalyst 3560-E Switches, and RPS 2300 Power Supply Modules*
- *Installation Notes for the Catalyst 3750-E and Catalyst 3560-E Switch Fan Module*
- *Installation Notes for the Cisco TwinGig Converter Module*
- *Cisco Redundant Power System 2300 Hardware Installation Guide*
- *Cisco Redundant Power System 2300 Compatibility Matrix*
- Device manager online help (available on the switch)

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*
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

For other information about related products, see these documents:

- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*
- *Network Admission Control Software Configuration Guide*

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.