



Release Notes for Catalyst 3750-X, 3750-E, 3560-X, and 3560-E Switches, Cisco IOS Release 12.2(58)SE1 and Later

Revised June 6, 2012



Note

Cisco IOS Release 12.2(58)SE images for all platforms were removed from Cisco.com because of a severe defect, CSCto62631. The solution for the defect is in Cisco IOS Release 12.2(58)SE1.

Cisco IOS Release 12.2(58)SE1 and later runs on Catalyst 3750-X, Catalyst 3750-E, Catalyst 3650-X, and Catalyst 3560-E switches and on Cisco enhanced EtherSwitch service modules.

The Catalyst 3750-X and 3750-E switches support stacking through Cisco StackWise Plus technology. The Catalyst 3750-X also supports StackPower. The Catalyst 3560-X switches, Catalyst 3650-E switches, and the Cisco enhanced EtherSwitch service modules do not support switch stacking.

Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack. Cisco enhanced EtherSwitch service modules and Catalyst 3560-E switches support the same features.

For more information, see the [Deciding Which Files to Use, page 9](#) and the “[Related Documentation](#)” section on page 48.

These release notes include important information about Cisco IOS Release 12.2(55)SE and later 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 9.
- 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 9.

You can download the switch software from this site (registered Cisco.com users with a login password): <http://www.cisco.com/cisco/software/navigator.html?a=http://www.cisco.com/cisco/web/download/index.htmli=rpm>



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

© 2011 Cisco Systems, Inc. All rights reserved.

**Note**

Upgrading the software image on a Catalyst 3560-X or 3750-X switch from Cisco IOS Release 12.2(53)SE2 or 12.2(55)SE to Cisco IOS Release 12.2(58)SE1 could take up to 20 minutes.

Contents

- “System Requirements” section on page 2
- “Upgrading the Switch Software” section on page 9
- “Installation Notes” section on page 13
- “New Software Features” section on page 13
- “Limitations and Restrictions” section on page 19
- “Important Notes” section on page 31
- “Open Caveats” section on page 33
- “Resolved Caveats” section on page 35
- “Documentation Updates” section on page 41
- “Related Documentation” section on page 48
- “Obtaining Documentation and Submitting a Service Request” section on page 50

System Requirements

- “Supported Hardware” section on page 2
- “Device Manager System Requirements” section on page 8
- “Cluster Compatibility” section on page 8
- “CNA Compatibility” section on page 8

Supported Hardware

Table 1 *Catalyst 3750-X and Catalyst 3560-X Supported Hardware*

Switch Model	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750-X-12S-S	12 SFP module slots, StackWise Plus, StackPower, 1 network module slot, 350-W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(58)SE1
Catalyst 3750-X-24S-S	24 SFP module slots, StackWise Plus, StackPower, 1 network module slot, 350-W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(58)SE1
Catalyst 3750-X-12S-E	12 SFP module slots, StackWise Plus, StackPower, 1 network module slot, 350-W power supply; IP Services feature set	Cisco IOS Release 12.2(58)SE1
Catalyst 3750-X-24S-E	24 SFP module slots, StackWise Plus, StackPower, 1 network module slot, 350-W power supply; IP Services feature set	Cisco IOS Release 12.2(58)SE1

Table 1 *Catalyst 3750-X and Catalyst 3560-X Supported Hardware (continued)*

Switch Model	Description	Supported by Minimum Cisco IOS Release
Catalyst 3750-X-24T-L	24 10/100/1000 Ethernet ports, StackWise Plus, 1 network module slot, 350 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-48T-L	48 10/100/1000 Ethernet ports, StackWise Plus, one network module slot, 350 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-24P-L	24 10/100/1000 PoE+ ² ports, StackWise Plus, 1 network module slot, 715 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-48P-L	48 10/100/1000 PoE+ ² ports, StackWise Plus, one network module slot, 715 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-48PF-L	48 10/100/1000 PoE+ ² ports, StackWise Plus, 1 network module slot, 1100 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-24T-S	24 10/100/1000 Ethernet ports, StackWise Plus, StackPower, 1 network module slot, 350 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-48T-S	48 10/100/1000 Ethernet ports, StackWise Plus, StackPower, 1 network module slot, 350 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-24P-S	24 10/100/1000 PoE+ ² ports, StackWise Plus, StackPower, 1 network module slot, 715 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-48P-S	48 10/100/1000 PoE+ ² ports, StackWise Plus, StackPower, 1 network module slot, 715 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3750-X-48PF-S	48 10/100/1000 PoE+ ² ports, StackWise Plus, StackPower, 1 network module slot, 1100 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-24T-L	24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-48T-L	48 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-24P-L	24 10/100/1000 PoE+ ² ports, 1 network module slot, 715 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-48P-L	48 10/100/1000 PoE+ ² ports, 1 network module slot, 715 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-48PF-L	48 10/100/1000 PoE+ ² ports, 1 network module slot, 1100 W power supply; LAN Base feature set	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-24T-S	24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-48T-S	48 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-24P-S	24 10/100/1000 PoE+ ² ports, 1 network module slot, 715 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-48P-S	48 10/100/1000 PoE+ ² ports, 1 network module slot, 715 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-X-48PF-S	48 10/100/1000 PoE+ ² ports, 1 network module slot, 1100 W power supply; IP Base feature set ¹	Cisco IOS Release 12.2(53)SE2

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

Switch Model	Description	Supported by Minimum Cisco IOS Release
C3KX-NM-10G 10-Gigabit Ethernet Network Module	Four SFP slots. Two slots support only 1-Gigabit SFP modules, two slots support either 1-Gigabit SFP or 10-Gigabit SFP+ modules.	Cisco IOS Release 12.2(53)SE2
C3KX-NM-1G 1-Gigabit Ethernet Network Module	Four 1-Gigabit SFP module slots	Cisco IOS Release 12.2(53)SE2
SFP Modules	100FX-SFP GE SFPLX/LH GE SFP SX 1000BASE-LX/LH 1000BASE-SX 1000BASE-ZX 1000BASE-BX10-D 1000BASE-BX10-U 1000BASE-T 100BASE-FX CWDM ³ DWDM ⁴ Note =For a complete list of supported SFP modules, see the hardware installation guide or the data sheets at: http://www.cisco.com/en/US/products/ps10745/products_data_sheets_list.html	Cisco IOS Release 12.2(53)SE2
SFP+ Modules	SFP-10G-SR SFP-10G-LR SFP-10G-LRM SFP-H10GB CU1M SFP-H10GB CU3M SFP-H10GB CU5M	Cisco IOS Release 12.2(53)SE2
Support for these SFP+ modules	Only version 02 (or later) of the CX1 ⁵ cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	Cisco IOS Release 12.2(53)SE2
SFP module patch cable ⁶	CAB-SFP-50CM	Cisco IOS Release 12.2(53)SE2
Power supply modules	C3KX-PWR-1100WAC C3KX-PWR-715WAC C3KX-PWR-350WAC C3KX-PWR-440WDC C3KX-PSBAY-BLNK Note For power supply module descriptions and configurations supported on switch models, see the hardware installation guide.	Cisco IOS Release 12.2(53)SE2
eXpandable power system (XPS)	Cisco XPS 2200	Cisco IOS Release 12.2(55)SE1 and later

1. Option to upgrade the IP Base feature set to IP Services feature set is available when ordering the switch

2. PoE+ = Power over Ethernet, up to 30 W per port
3. CWDM = coarse wavelength-division multiplexer
4. DWDM = dense wavelength-division multiplexer
5. The CX1 cables are used with the OneX converters.
6. Only Catalyst 3560-X 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 be used in 1 Gigabit Ethernet SFP ports to connect two Catalyst 3560-X switches in a cascaded configuration. You can use the patch cable with the 10 G network module only on SFP ports 1 and 3 (not on SFP+ ports 2 and 4).

Table 2 *Catalyst 3750-E and 3560-E Switches and Cisco Enhanced EtherSwitch Service Module 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
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

Table 2 *Catalyst 3750-E and 3560-E Switches and Cisco Enhanced EtherSwitch Service Module Supported Hardware (continued)*

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
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 10 Gigabit Ethernet X2 ZR optical modules	Cisco IOS Release 12.2(35)SE2 Cisco IOS Release 12.2(40)SE Cisco IOS Release 12.2(50)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 SFP-10G-SR SFP-10G-LR For a complete list of supported SFPs and part numbers, see the data sheet: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps7077/product_data_sheet0900aecd805bbe67.html	Cisco IOS Release 12.2(35)SE2 Cisco IOS Release 12.2(53)SE
DOM ⁴ support for these SFP modules.	X2-10GB-ER, X2-10GB-SR, X2-10GB-LR, X2-10GB-LRM, X2-10GB-ZR GLC-ZX-SM, GLC-BX-D, GLC-BX-U SFP-GE-S, SFP-GE-L, SFP-GE-Z All CWDM and DWDM SFP modules	Cisco IOS Release 12.2(46)SE
SFP module patch cable ⁵	CAB-SFP-50CM	Cisco IOS Release 12.2(35)SE2
Supports OneX (CVR-X2-SFP10G) and these SFP+ modules	SFP-10G-SR= SFP-10G-LR= SFP-10G-LRM= Only version 02 or later CX1 ⁶ cables support these SFP modules: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	12.2(53)SE

Table 2 *Catalyst 3750-E and 3560-E Switches and Cisco Enhanced EtherSwitch Service Module Supported Hardware (continued)*

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
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
SM-D-ES2-48 ⁷	48 10/100 ports, 2 SFP module slots	12.2(52)EX
SM-D-ES3-48-P ⁷	48 10/100 ports with PoE, 2 SFP module slots	12.2(52)EX
SM-D-ES3G-48-P ⁷	48 10/100/1000 with PoE, 2 SFP module slots	12.2(52)EX
SM-ES2-16-P ⁷	15 10/100 ports with PoE, 1 10/100/1000 port with PoE	12.2(52)EX
SM-ES2-24 ⁷	23 10/100 ports, 1 10/100/1000 port	12.2(52)EX
SM-ES2-24-P ⁷	Layer 2-capable, 23 10/100 ports with PoE, 1 10/100/1000 port with PoE	12.2(52)EX
SM-ES3-16-P ⁷	15 10/100 ports with PoE, 1 10/100/1000 port with PoE	12.2(52)EX
SM-ES3-24-P ⁷	23 10/100 ports with PoE, 1 10/100/100 port with PoE	12.2(52)EX
SM-ES3G-16-P ⁷	16 10/100/1000 ports with PoE	12.2(52)EX
SM-ES3G-24-P ⁷	24 10/100/1000 ports with PoE	12.2(52)EX

- PoE = Power over Ethernet.
- SFP = small form-factor pluggable
- CWDM = coarse wavelength-division multiplexer
- DOM = digital optical monitoring
- 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.
- The CX1 cables are used with the OneX converter and are supported in Cisco IOS Release 12.2(53)SE and later.
- Cisco enhanced EtherSwitch service module

Device Manager System Requirements

Hardware

Table 3 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 6.0, 7.0, Firefox 1.5, 2.0 or later with JavaScript enabled.

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

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-X switch, all standby command switches must be Catalyst 3750-X switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant*, *Release Notes for Cisco Network Assistant*, the Cisco enhanced EtherSwitch service module documentation, the software configuration guide, and the command reference.

CNA Compatibility

Cisco IOS 12.2(55)SE will be supported in a future release of the Cisco Network Assistant. Cisco IOS 12.2(35)SE2 and later is only compatible with Cisco Network Assistant 5.0 and later. You can download Cisco Network Assistant from this URL:

<http://www.cisco.com/cisco/software/navigator.html?mdfid=279230132http://www.cisco.com/cgi-bin/tablebuild.pl/NetworkAssistanti=rp>

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

Upgrading the Switch Software

- “Finding the Software Version and Feature Set” section on page 9
- “Deciding Which Files to Use” section on page 9
- “Archiving Software Images” section on page 11
- “Upgrading a Switch by Using the Device Manager or Network Assistant” section on page 12
- “Upgrading a Switch by Using the CLI” section on page 12
- “Recovering from a Software Failure” section on page 13

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 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

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image and a specific software license. If you do not have a service support contract, such as a SMARTnet contract, download the IP base image from Cisco.com. For Catalyst 3750-X and 3560-X switches, this image has the IP base and LAN base feature sets. For Catalyst 3750-E and 3560-E switches, this image has the IP base feature set.



Note

A Catalyst 3750-X or 3560-X switch running the LAN base feature set supports only 255 VLANs.

The switches running the universal software images can use permanent and temporary software licenses. See the “Cisco IOS Software Activation Conceptual Overview” chapter in the *Cisco IOS Software Activation Configuration Guide*:

http://www.cisco.com/en/US/docs/ios/csa/configuration/guide/12.4T/csa_book.html

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 Catalyst 3750-E and 3560-E software activation, see the *Cisco Software Activation and Compatibility Document* on Cisco.com:

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

Catalyst 3750-X and 3560-X switches running payload-encryption images can encrypt management and data traffic. Switches running nonpayload-encryption images can encrypt only management traffic, such as a Secure Shell (SSH) management session.

- Management traffic is encrypted when SSH, Secure Socket Layer (SSL), Simple Network Management Protocol (SNMP), and other cryptographic-capable applications or protocols are enabled.
- Data traffic is encrypted when MACsec is enabled.

For more information about Catalyst 3750-X and 3560-X software licenses and available images, see the *Cisco IOS Software Installation Document* on Cisco.com:

http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

Table 4 **Software Images**

Image	Filename	Description
Catalyst 3750-X and Catalyst 3560-X switches		
IP base without payload encryption	c3750e-ipbasek9npe-tar.122-58.SE1.tar c3560e-ipbasek9npe-tar.122-58.SE1.tar	Layer 2 and basic Layer 3 features, SSH ¹ , SSL ² , and SNMPv3 ³ , and Kerberos IP base image, as well as LAN base image with Layer 2 features
IP base with payload encryption	c3750e-ipbasek9-tar.122-58.SE1.tar c3560e-ipbasek9-tar.122-58.SE1.tar	Layer 2 and basic Layer 3 features, SSH, SSL, SNMPv3, Kerberos, and MACsec ⁴ IP base image, as well as LAN base image with Layer 2 features
Universal without payload encryption	c3750e-universalk9npe-tar.122-58.SE1.tar c3560e-universalk9npe-tar.122-58.SE1.tar	All the supported universal image features, Kerberos, SSH, SSL, and SNMPv3 LAN base, IP base, and IP services software licenses
Universal with payload encryption	c3750e-universalk9-tar.122-58.SE1.tar c3560e-universalk9-tar.122-58.SE1.tar	All the supported universal image features, Kerberos, SSH, SSL, SNMPv3, and MACsec LAN base, IP base, and IP services software licenses
Catalyst 3750-E and Catalyst 3560-E switches		
IP base image	c3750e-ipbasek9-tar.122-58.SE1.tar c3560e-ipbasek9-tar.122-58.SE1.tar	Layer 2 and basic Layer 3 features, SSH, SSL, SNMPv3, and Kerberos
Universal image	c3750e-universalk9-tar.122-58.SE1.tar c3560e-universalk9-tar.122-58.SE1.tar	All the supported universal image features, Kerberos, SSH, SSL, and SNMPv3 IP base and IP services software licenses
Cisco enhanced EtherSwitch service modules		

Table 4 **Software Images (continued)**

Image	Filename	Description
LAN base image	c2960-lanbasek9-tar.122-58.SE1.tar	Layer 2 features, SSH, SNMPv3, and Kerberos For these service modules: SM-D-ES2-48, SM-ES2-16-P, SM-ES2-24, and SM-ES2-24-P6.
Universal image	c3560e-universalk9-tar.122-58.SE1.tar	All the supported universal image features, Kerberos, SSH, SSL, and SNMPv3 IP base and IP services software licenses For these service modules: SM-D-ES3-48-P, SM-D-ES3G-48-P, SM-ES3-16-P, SM-ES3-24-P, SM-ES3G-16-P, and SM-ES3G-24-P.

1. SSH = Secure Shell
2. SSL = Secure Socket Layer
3. SNMPv3 = Simple Network Management Protocol Version 3
4. MACsec = MAC security standard

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.

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*:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.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 10](#) to identify the file that you want to download.
- Step 2** Download the software image file:
 - a. If you are a registered customer, go to this URL and log in:
<http://www.cisco.com/cisco/software/navigator.html?a=http://www.cisco.com/cisco/web/download/index.html&rpm>
 - b. Navigate to **Switches > LAN Switches - Access**
 - c. Navigate to your switch model.
 - d. Click **IOS Software**, then select the latest IOS release.
 - e. 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 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/c3750x-universal-tar.122-55.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 recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

Use these methods to assign IP information to your switch:

- 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 Software Features

- Support for the Built-in Traffic Simulator using Cisco IOS IP SLAs video operations to generate synthetic traffic for a variety of video applications, such as Telepresence, IPTV, and IP video surveillance cameras. You can use the simulator tool:
 - for network assessment before deploying applications with stringent network performance requirements.
 - with Cisco Mediatrace for post-deployment troubleshooting of network-related performance issues.

The traffic simulator includes a sophisticated scheduler that allows you to run several tests simultaneously or periodically, and over extended time periods.

- The command ‘ip tcp adjust-mss’ is not supported on the 3750x/3560x/3750g/3560g/3750e/3560e platforms.
- Cisco Mediatrace to troubleshoot and isolate network or application issues in traffic streams. It helps drill down to analyze one-way delay, one-way packet loss, one-way jitter, and connectivity in IPv4 networks that carry video traffic. You can use Mediatrace for any UDP-based video or non-video traffic stream.

- Cisco Application Performance Monitor to track the video packet flow and to troubleshoot and isolate performance degradation in traffic streams. You can use the performance monitor for both video and non-video traffic.
- EnergyWise Phase 2.5 enhancements that add support for a query to analyze and display domain information and for Wake on LAN (WoL) to remotely power on a WoL-capable PC.
- Smart logging to capture and export packet flows to a NetFlow collector. This release supports smart logging for DHCP snooping or dynamic ARP inspection violations, IP source guard denied traffic, and ACL traffic permitted or denied on Layer 2 ports.
- Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate
- VACL Logging to generate syslog messages for ACL denied IP packets
- Smart Install enhancements including the ability to manually change a client switch health state from denied to allowed or hold for on-demand upgrades, to remove selected clients from the director database, to allow simultaneous on-demand upgrade of multiple clients, and to provide more information about client devices, including device status, health status, and upgrade status.
- AutoSmartports enhancement to enable auto-QoS on a CDP-capable Cisco digital media player.
- Memory consistency check routine enhancements to detect and correct invalid ternary content addressable memory (TCAM) table entries that can affect switch performance
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.
- Support for 16 static routes on switch virtual interfaces (SVIs) on Catalyst 3750-X or 3560-X switches running the LAN base image.
- Introduction of a new switch database management (SDM) dual IPv4 and IPv6 template that supports more indirect routes.
- IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates to support the IP version 6 (IPv6)-only and the IPv6 part of the protocol-version independent (PVI) objects and tables.
- Network Time Protocol version 4 (NTPv4) to support both IPv4 and IPv6 and compatibility with NTPv3.
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).
- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent.
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- Rolling stack upgrade to minimize network disruption when the members of a switch stack are upgraded one at a time (Catalyst 3750X and 3750E only).
- NSF IETF mode for OSPFv2—OSPFv2 graceful restart support for IPv4. (IP services feature set only)
- NSF IETF mode for OSPFv3—OSPFv3 graceful restart support for IPv6. (IP services feature set only)
- Support for the Virtual Router Redundancy Protocol (VRRP) for IPv4, which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address.
- Support for deny ACL entries in Web Cache Communication Protocol (WCCP) redirect lists. Previously only permit entries were supported.

Minimum Cisco IOS Release for Major Features

Table 5 lists the minimum software release after the first release of required to support the major features on the switches. The first release of the Catalyst 3750-X and 3560-X switches was Cisco IOS Release 12.2(53)SE2).

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

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Built-in Traffic Simulator using Cisco IOS IP SLAs video operations	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Cisco Mediatrace support	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Cisco performance monitor	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
EnergyWise Phase 2.5	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Smart logging	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Protocol storm protection	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
VACL Logging	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Smart Install 3.0	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Auto Smartports enhancements to enable auto-QoS on a digital media player.	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Memory consistency check routines	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Call Home support	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Support for 16 static routes on SVIs on the LAN Base feature set	12.2(58)SE1	3750-X, 3560-X
SDM template supporting more indirect routes	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
NTP version 4	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
DHCPv6 bulk-lease query and DHCPv6 relay source configuration	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Rolling stack upgrade	12.2(58)SE1	3750-X, 3750-C
NSF IETF mode for OSPFv2 and OSPFv3 (IP services feature set)	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
RADIUS, TACACS+, and SSH/SCP over IPv6	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X

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
VRRP for IPv4	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates	12.2(58)SE1	3750-E, 3560-E 3750-X, 3560-X
Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices.	12.2(55)SE	3750-E, 3560-E 3750-X, 3560-X
AutoSmartports enhancements—support for global macros, last-resort macros, event trigger control, access points, EtherChannels, auto-QoS with Cisco Medianet, and IP phones.	12.2(55)SE	3750-E, 3560-E 3750-X, 3560-X
CDP and LLDP enhancements for exchanging location information with video end points.s.	12.2(55)SE	3750-E, 3560-E 3750-X, 3560-X
Smart Install enhancements including client backup files, zero-touch replacement for clients with the same product-ID, and automatic generation of the image_list file.	12.2(55)SE	3750-E, 3560-E 3750-X, 3560-X
Dynamic creation or attachment of an auth-default ACL on a port with no configured static ACLs.	12.2(55)SE	3750-E, 3560-E 3750-X, 3560-X
VLAN assignment on a port configured for multi-auth mode.	12.2(55)SE	3750-E, 3560-E 3750-X, 3560-X
EEM in IP base image.	12.2(55)SE	3750-E, 3560-E 3750-X, 3560-X
IP base support for OSPF routed access.	12.2(55)SE	3750-E, 3560-E 3750-X, 3560-X
Cisco TrustSec SXP.	12.2(55)SE 12.2(53)SE2	3750-E, 3560-E 3750-X, 3560-X
Cisco EnergyWise Phase 2 to manage power usage of EnergyWise-enabled Cisco devices and non-Cisco end points running EnergyWise agents ¹	12.2(53)SE1	3750-E, 3560-E
AutoSmartports enhancements (macro persistency, LLDP-based triggers, MAC address and OUI-based triggers.	12.2(52)SE	3750-E, 3560-E
EEM 3.2 Neighbor Discovery, Identity, and MAC-Address-Table.	12.2(52)SE	3750-E, 3560-E
Support for IP source guard on static hosts.	12.2(52)SE	3750-E, 3560-E
RADIUS Change of Authorization (CoA).	12.2(52)SE	3750-E, 3560-E
802.1x User Distribution to allow deployments with multiple VLANs.	12.2(52)SE	3750-E, 3560-E
Critical VLAN with multiple-host authentication.	12.2(52)SE	3750-E, 3560-E
Customizable web authentication enhancement.	12.2(52)SE	3750-E, 3560-E
Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.	12.2(52)SE	3750-E, 3560-E
VLAN-ID based MAC authentication.	12.2(52)SE	3750-E, 3560-E
MAC move to allow hosts to move across ports within the same switch without any restrictions to enable mobility.	12.2(52)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
SNMPv3 with Triple Data Encryption Standard (3DES) and 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms.	12.2(52)SE	3750-E, 3560-E
Hostname inclusion in the option 12 field of DHCPDISCOVER packets.	12.2(52)SE	3750-E, 3560-E
DHCP Snooping enhancement to support the circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE	3750-E, 3560-E
LLPD-MED enhancements to allow the switch to grant power to the power device (PD), based on the power policy TLV request.	12.2(52)SE	3750-E, 3560-E
VTP version 3 support.	12.2(52)SE	3750-E, 3560-E
QoS marking of CPU-generated traffic and queue CPU-generated traffic on egress ports.	12.2(52)SE	3750-E, 3560-E
NEAT with 802.1X switch supplicant, host authorization with CISP, and auto enablement	12.2(52)SE	3750-E, 3560-E
802.1x with open access.	12.2(52)SE	3750-E, 3560-E
802.1x authentication with downloadable ACLs and redirect URLs.	12.2(52)SE	3750-E, 3560-E
Flexible-authentication sequencing to configure the order of authentication methods tried by a port.	12.2(52)SE	3750-E, 3560-E
Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port	12.2(52)SE	3750-E, 3560-E
Supports the LLPD-MED MIB and the CISCO-ADMISSION-POLICY MIB.	12.2(52)SE	3750-E, 3560-E
Full QoS support for IPv6 traffic.	12.2(50)SE	3750-E, 3560-E
Smart Install to allow a single point of management (director) in a network.	12.2(50)SE	3750-E, 3560-E
Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications.	12.2(50)SE	3750-E, 3560-E
Support for up to 32 10 Gigabit Ethernet DWDM X2 optical modules.	12.2(52)SE	3750-E, 3560-E
Wired location service.	12.2(50)SE	3750-E, 3560-E
Intermediate System-to-Intermediate System (IS-IS) routing for Connectionless Network Service (CLNS) networks	12.2(50)SE	3750-E, 3560-E
Stack troubleshooting enhancements	12.2(50)SE	3750-E
Support for the Cisco IOS Configuration Engine (previously the Cisco IOS CNS agent)	12.2(50)SE	3750-E, 3560-E
Embedded Event Manager Version 2.4	12.2(50)SE	3750-E, 3560-E
LLDP-MED network-policy profile time, length, value (TLV).	12.2(50)SE	3750-E, 3560-E
RADIUS server load balancing.	12.2(50)SE	3750-E, 3560-E
Auto Smartports Cisco-default and user-defined macros.	12.2(50)SE	3750-E, 3560-E
Support for these MIBs: SCP attribute in the CONFIG_COPY MIB, CISCO-AUTH-FRAMEWORK, CISCO-MAC-AUTH-BYPASS, LLDP	12.2(50)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
IPv6 features supported in the IP services and IP base software images: ACLs; DHCPv6 for the DCHP server, client, and relay device; EIGRPv6; HSRPv6; OSPFv3; RIP; Static routes	12.2(50)SE	3750-E, 3560-E
Generic message authentication support with the SSH Protocol and compliance with RFC 4256	12.2(50)SE	3750-E, 3560-E
Voice aware 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 calculation	12.2(46)SE	3750-E, 3560-E
HSRP Version 2 (HSRPv2)	12.2(46)SE	3750-E, 3560-E
HSRP for IPv6 (requires the 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
Rehosting a software license and 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 (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 services 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
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
/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

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
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

1. Cisco enhanced EtherSwitch service modules do not support Cisco EnergyWise.

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

- “Access Control List” section on page 20
- “Address Resolution Protocol” section on page 20
- “Cisco Transceiver Modules and SFP Modules” section on page 21
- “Configuration” section on page 21
- “EtherChannel” section on page 22
- “IEEE 802.1x Authentication” section on page 23
- “Multicasting” section on page 24
- “PoE or PoE+” section on page 24
- “QoS” section on page 25
- “RADIUS” section on page 26
- “Routing” section on page 26
- “SPAN and RSPAN” section on page 27
- “Stacking (only Catalyst 3750-X and Catalyst 3750-E Switch Stack)” section on page 27
- “Stack Power (Catalyst 3750-X only)” section on page 29
- “VLANs” section on page 29

Access Control List

- 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

- 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

- 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 Transceiver Modules and SFP Modules

- (Catalyst 3750-E or 3560-E switches) 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)
- (Catalyst 3750-E or 3560-E switches) 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

- If a half-duplex port running at 10 Mb/s receives frames with Inter-Packet Gap (IPG) that do not conform to Ethernet specifications, the switch might stop sending packets.

There is no workaround. (CSCec74610) (Catalyst 3750-X switches)

- 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)

- (Catalyst 3750-X or 3750-E switches) If you enter the **show tech-support** privileged EXEC command after you enter the **remote command {all | stack-member-number}** privileged EXEC command, the complete output does not appear.

The workaround is to use the **session stack-member-number** privileged EXEC command. (CSCsz38090)

- (Catalyst 3750-X or 3560-X switches) When the switch flash memory has less than 6 MB free space, there is not enough space in flash memory to hold temporary files created as part of a microcontroller unit (MCU) image upgrade, and the upgrade fails.

The workaround is to delete any unnecessary files in flash memory, delete the temporary files created as part of the failed upgrade, and try the MCU upgrade again. (CSCtd75400)

Diagnostics

- (Catalyst 3750-X or 3560-X switches) When you enter the **test cable-diagnostics tdr interface** or the **show cable-diagnostics tdr interface** privileged EXEC command on an interface to determine the length of a connected cable, the cable length might be reported as N/A. This can occur when there is no link, a 10 Mb/s link, or a 100 Mb/s link, even though there are no cable faults. Cable length is reported correctly when a 1 Gb/s link is active on the interface.

The workaround to verify the cable length is to enter the commands when a Gigabit link is active on the interface or after disconnecting the far end of the cable. (CSCte43869)

EtherChannel

- 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

- 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

- 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 or PoE+

- 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)

- (Catalyst 3750-X or 3560-X switches) When a powered device (such as an IP phone) connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the switch locks to the power-negotiation protocol of that first packet. The switch does not respond to power requests from the other protocol. For example, if the switch is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the switch has locked on it, the switch does not respond to LLDP power requests and can no longer power on any accessories.

The workaround is to turn the powered device off and then on again.

QoS

- 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)

- If QoS is enabled on a switch and the switch has a high volume of incoming packets with a maximum transmission unit (MTU) size greater than 1512 bytes, the switch might reload.

Use one of these workarounds:

- Use the default buffer size.
- Use the **mls qos queue-set output qset-id buffers allocation1 ... allocation4** global configuration command to allocate the buffer size. The buffer space for each queue must be at least 10 percent. (CSCsx69718) (Catalyst 3750-X switches)

- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

```
01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
```

There is no impact to switch functionality.

There is no workaround. (CSCtg32101)

RADIUS

- RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN. There is no workaround. (CSCta05071)

Routing

- 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)

Smart Install

- When upgrading switches in a stack, the director cannot send the correct image and configuration to the stack if all switches in the stack do not start at the same time. A switch in the stack could then receive an incorrect image or configuration.

The workaround is to use an on-demand upgrade to upgrade switches in a stack by entering the **vstack download config** and **vstack download image** commands. (CSCta64962)

- When you upgrade a Smart Install director to Cisco IOS Release 12.2(55)SE but do not upgrade the director configuration, the director cannot upgrade client switches.

When you upgrade the director to Cisco IOS Release 12.2(55)SE, the workaround is to also modify the configuration to include all built-in, custom, and default groups. You should also configure the tar image name instead of the image-list file name in the stored images. (CSCte07949)

- Backing up a Smart Install configuration could fail if the backup repository is a Windows server and the backup file already exists in the server.

The workaround is to use the TFTP utility of another server instead of a Windows server or to manually delete the existing backup file before backing up again. (CSCte53737)

- In a Smart Install network with the backup feature enabled (the default), the director sends the backup configuration file to the client during zero-touch replacement. However, when the client is a switch in a stack, the client receives the seed file from the director instead of receiving the backup configuration file.

The workaround, if you need to configure a switch in a stack with the backup configuration, is to use the **vstack download config** privileged EXEC command so that the director performs an on-demand upgrade on the client.

- When the backup configuration is stored in a remote repository, enter the location of the repository.
- When the backup file is stored in the director flash memory, you must manually set the permissions for the file before you enter the **vstack download config** command. (CSCtf18775)
- If the director in the Smart Install network is located between an access point and the DHCP server, the access point tries to use the Smart Install feature to upgrade even though access points are not supported devices. The upgrade fails because the director does not have an image and configuration file for the access point.

There is no workaround. (CSCtg98656)

- When a Smart Install director is upgrading a client switch that is not Smart Install-capable (that is, not running Cisco IOS Release 12.2(52)SE or later), the director must enter the password configured on the client switch. If the client switch does not have a configured password, there are unexpected results depending on the software release running on the client:
 - When you select the NONE option in the director CLI, the upgrade should be allowed and is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.
 - When you enter any password in the director CLI, the upgrade should not be allowed, but it is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.

There is no workaround. (CSCth35152)

SPAN and RSPAN

- 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)

- (Catalyst 3750-E or 3560-E switches) The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

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

- (Catalyst 3650-X and 3750-X switches) When you enter the **show monitor** privileged EXEC command, the monitor source port output is incorrect. This situation occurs when the monitor source port is a pluggable Gigabit module and you set any source port combination. This error does not occur when you use a single Gigabit port on the pluggable module as the source port.

The workaround is to use the **show platform monitor session** privileged EXEC command to display the correct source ports. (CSCtn67868)

Stacking (only Catalyst 3750-X and Catalyst 3750-E Switch Stack)

- When a switch stack is running 802.1x single host mode authentication and has filter-ID or per-user policy maps applied to an interface, these policies are removed if a master switchover occurs. Even though the output from the **show ip access-list** privileged EXEC command includes these ACLs, the policies are not applied.

The workaround is to enter a **shutdown** and then a **no shutdown** interface configuration command on the interface. (CSCsx70643)

- Where there is a mixed hardware stack with Catalyst 3750-X or 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-X or 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-X or 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-X or 3750-E switches, when the stack reloads, the Catalyst 3750-X or 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)

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

- You configure a Layer 2 protocol tunnel port on the master switch.
- You configure a Layer 2 protocol tunnel port on the member switch.
- You add the port channel to the Layer 2 protocol tunnel port on the master switch.
- 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 (CSCsk96058)
```

- 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)

- When the switch stack is in the HSRP active state and a master changeover occurs, you cannot ping the stack by using an HSRP virtual IP address.

There is no workaround. (CSCth00938)

- In a stackable switch, if VRF configuration is changed and this is followed by a master switchover, VRF stops working.

The workaround is to reload the switch stack after the VRF configuration is changed. (CSCtn71151)

Stack Power (Catalyst 3750-X only)

- When a power stack has been configured in redundant mode, which is not the default, and then split by either removing cables or disabling StackPower ports, the newly created power stack has the same mode as the former power stack, but this is not shown in the configuration file.

The workaround when you are forming power stack topologies if the power stack mode is not the default (power sharing), you should also configure the power stack mode on the new power stacks by entering the **mode redundant** power-stack configuration command. (CSCte33875)

VLANs

- 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)

- 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)

- 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. (CSCsk65142)

- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

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

- [“Switch Stack Notes” section on page 31](#)
- [“Cisco IOS Notes” section on page 31](#)
- [“Device Manager Notes” section on page 32](#)

Switch Stack Notes

- Always power off a switch before adding or removing it from a switch stack.
- The Catalyst 3560-X and 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

- Unlike other platforms, the response to an Energywise query on a Catalyst 3750-X or 3560-X is the actual switch power consumption and not a fixed number.
- 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, 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

- 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.

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. <ul style="list-style-type: none"> • 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

Unless otherwise noted, these caveats apply to Catalyst 3750-X, 3750-E, 3560-X, and 3560-E switches:

- CSCte99366

In a Smart Install network, when the director is connected between the client and the DHCP server and the server has options configured for image and configuration, then the client does not receive the image and configuration files sent by the DHCP server during an automatic upgrade. Instead the files are overwritten by the director and the client receives the image and configuration that the director sends.

Use one of these workarounds:

- If client needs to upgrade using an image and configuration file configured in the DHCP server options, you should remove the client from the Smart Install network during the upgrade.
- In a network using Smart Install, you should not configure options for image and configuration in the DHCP server. For clients to upgrade using Smart Install, you should configure product-id specific image and configuration files in the director.

- CSCtf79259 (Catalyst 3750-X or 3560-X switches)

If you install 10/100/1000BASE-TX or 100BASE-FX SFPs in the SFP+ module ports (port 2 or port 4), the ports are put in an error disabled state. These SFPs are not supported in the SFP+ ports.

There is no workaround.

- CSCtg35226 (Catalyst 3750-X or 3750-E switches)

Cisco Network Assistant displays the LED ports with a light blue color for all switches in a stack that have the Catalyst 3750G-48PS switch as part of the stack.

There is no workaround.

- CSCtg98453

When you make port security changes on an interface, such as configuring aging time, violations, or aging type, error messages and tracebacks might appear.

There is no workaround.

- CSCtj97806

Mediatrace does not report statistics on the initiator under these conditions:

- The responder is a mixed switch stack with a Catalyst 3750 as the master switch
- The ingress interface on the responder from the initiator is on a member switch.

The workaround is to ensure that the mediatrace ingress and egress connections are on the stack master or to configure a Catalyst 3750-E or 3750-X as the stack master and then reload the switch stack.

- CSCtl32991

Unicast EIGRP packets destined for the switch are sent to the host queue instead of to the higher priority routing protocol queue.



Note This does not occur when packets are routed through the switch to another destination.

There is no workaround.

- CSCtl60247

When a switch or switch stack running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. If the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

There is no workaround.

- CSCtl81217

When a switch is using a DHCP server to assign IP addresses and an interface on the switch has RIP enabled, if the switch reloads, the interface loses some RIP configuration (specifically RIP authentication mode and RIP authentication key-chain). This does not happen when the IP address is statically configured on the interface. The problem occurs only when you configure RIP before an IP address is assigned by the DHCP server.

There is no workaround, but you can use an embedded event manager (EEM) script to add the interface configuration commands on the interface:

ip rip authentication mode

ip rip key-chain

- CSCtn49131 (Catalyst 3750-X and 3560-X)

When you enter the **show sdm template** privileged EXEC command on a switch running the LAN base feature set, incorrect values are displayed for vlan, routed interfaces and indirect IPv4 routes.

- The displayed values are: 8 routed interfaces, 1024 VLANs, 2K indirect IPv4 Routes
- The actual values are: 0 routed interfaces, 255 VLANs, 16 indirect IPv4 routes

There is no workaround.

- CSCto41442 (Catalyst 3750-X and 3750-E)

When you configure OSPFv3 graceful restart on a stack of switches with more than one OSPF area and you use the **router-id ip-address** router configuration command to configure a fixed router ID, if there is a switchover of the stack master switch, OSPFv3 graceful restart might be terminated.

The workaround, if possible, is to not use the **router-id** command to configure a fixed router ID with OSPFv3 graceful restart.

- CSCty02174 (Catalyst 3750-X)

A stack power member switch that does not have a PSU connected in Slot A or Slot B might fail during a Cisco IOS upgrade.

The workaround is to ensure that each stack member has at least one PSU connected. Alternatively, you can download and install the Cisco IOS image using the **archive download-sw /force-ucode-reload** privileged EXEC command.

Resolved Caveats

- [Caveats Resolved in Cisco IOS Release 12.2\(55\)SE4, page 35](#)
- [Caveats Resolved in Cisco IOS Release 12.2\(58\)SE2, page 36](#)
- [Caveats Resolved in Cisco IOS Release 12.2\(58\)SE1, page 36](#)

Caveats Resolved in Cisco IOS Release 12.2(55)SE4

- CSCtj83964

On a switch running Protocol-Independent Multicast (PIM) and Source Specific Multicast (SSM), multicast traffic might not be sent to the correct port after the switch reloads.

The workaround is to enter the **clear ip route** privileged EXEC command or reconfigure PIM and SSM after a reload.

- CSCtl51859

Neighbor discovery fails for IPv6 hosts connected to the switch when the IPv6 MLD snooping feature is enabled globally on the switch.

The workaround is to disable IPv6 MLD snooping on the switch.

Caveats Resolved in Cisco IOS Release 12.2(58)SE2

- CSCto07919

Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain.

These vulnerabilities are:

- Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
- ICMPv6 Packet May Cause MPLS-Configured Device to Reload

Cisco has released free software updates that address these vulnerabilities.

Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml>.

- CSCtq01926

When you configure a port to be in a dynamic VLAN by entering the **switchport access vlan dynamic** interface configuration command on it, the switch might reload when it processes ARP requests on the port.

The workaround is to configure static VLANs for these ports.

- CSCtq58248 (Catalyst Switch 3560-E)

On a Cisco Integrated Services Router with an Enhanced EtherSwitch Module (ES3), after upgrading the Cisco IOS release on the EtherSwitch Module to Release 12.2(58)SE1, the internal trunk link between the EtherSwitch and the router no longer passes any traffic.

The workaround is to upgrade to Cisco IOS Release 12.2(58)SE2.

Caveats Resolved in Cisco IOS Release 12.2(58)SE1

- CSCsz18045 (Catalyst 3750-E and 3560-E)

When you enter the **show inventory** command on a switch that has an X2 module, the output incorrectly reports the X2 module version ID (VID) as V01 even though the label has a higher VID.

There is no workaround.

- CSCtc72940 (Catalyst 3750-X and 3750-E)

When you reload a stack master, the **ip vrf forwarding** command does not appear in the running configuration, which causes AAA authentication to fail. This issue does not occur with standalone switches.

The workaround is to reenter the **ip vrf forwarding** command.

- CSCtd49241 (Catalyst 3560E-12SD and 3560E-12D switches)

When a Cisco Catalyst 3560E-12D or 3560E-12SD switch receives packets on an interface of a 10GBASE-SR or X2-10GB-LR module that is directly connected to a server, packets can be intermittently dropped after the server is restarted.

The workaround is to use the **shutdown** and **no shutdown** interface configuration commands on the interface.

- CSCtf21181 (Catalyst 3570-E switches)

A switch stack configured as a multicast router has a hardware programming error. Some multicast streams are not forwarded to a receiver while other streams from the same source are forwarded correctly. The unforwarded streams are Layer 2 forwarded by the stack on the same VLAN on which they were received to the multicast designated router for the VLAN.

The workaround is to use the **clear ip mroute** privileged EXEC command to resolve the hardware programming error.

- CSCtg00542

A Link Aggregation Control Protocol (LACP) bundle takes up to 70 seconds to form when NetFlow sampling is enabled.

The workaround is to disable NetFlow sampling.

- CSCtg11547

When you configure a switch to send messages to a syslog server in a VPN Routing and Forwarding (VRF) instance, the messages are not sent to the server.

The workaround is to remove the VRF configuration.

- CSCtg71149

When ports in an EtherChannel are linking up, the message `EC-5-CANNOT_BUNDLE2` might appear. This condition is often self-correcting, indicated by the appearance of `EC-5-COMPATIBLE` message following the first message. On occasion, the issue does not self-correct, and the ports may remain unbundled.

The workaround is to reload the switch or to restore the EtherChannel bundle by shutting down and then enabling the member ports and the EtherChannel in this order:

- Enter the **shutdown** interface configuration command on each member port.
- Enter the **shutdown** command on the port-channel interface.
- Enter the **no shutdown** command on each member port.
- Enter the **no shutdown** command on the port-channel interface.

- CSCth44403 (Catalyst 3750-E switch)

When you connect a switch as a VLAN Trunk Protocol (VTP) client to a Catalyst 4000 switch configured as a VTP client or server and the VTP database contains more than 512 VLANs, the database is not correctly updated.

The workaround is to connect the VTP client directly to a Catalyst 6500 VTP server.

- CSCth71862 (Catalyst 3750-X and 3750-E)

A host switch connected to a stack member switch can download a downloadable access control list (dACL) with more than 13 access control entries, but the dACL is not applied to an interface.

There is no workaround.

- CSCti07994 (Catalyst 3750-E and 3560-E)

When a Catalyst 3750-E or 3560-E switch has a 10/100/1000BASE-TX SFP module installed in a TwinGig SFP Converter Module, and you configure the SFP module to send at 100 Mb/s, save the configuration, and reload the switch, the speed setting is not saved to the running configuration.

There is no workaround.

- CSCti20222 (Catalyst 3750-X and 3750-E)
On a stack member, the **show interface** command output incorrectly displays a media-type setting. There is no workaround. This is a cosmetic error and does not affect the functionality of the switch.
- CSCti27620 (Catalyst 3750-X)
The switch does not generate SNMP traps when a power supply is disconnected. There is no workaround.
- CSCti37197
Enabling the Cisco Discovery Protocol (CDP) on a tunnel interface causes the switch to fail when a CDP packet is received on the interface.



Note Tunnels are not supported on these platforms.

The workaround is to use the **no cdp enable** interface configuration command to disable CDP on the interface.

- CSCti45352
When a FlexLinks backup interface is configured on a member switch in a switch stack, the backup interface incorrectly shows that all VLANs are in the forwarding state.
The workaround is to use the **show interface trunk** interface configuration command to display the status of the backup link.
- CSCti50576 (Catalyst 3760-X and 3560-X)
When traffic is passing through a port, if you unplug the port cable and then plug it back in, the LED might turn to black or might continue flashing amber.
The workaround is to wait until traffic stops passing through the port. The LED changes to the correct color and continues working normally.
- CSCti61145 (Catalyst 3750-E and 3560-E)
When you configure storm control with a range command on two interfaces that belong to an EtherChannel group, this message appears:

```
%SYS-3-CPUHOG: Task is running for (2097)msecs, more than (2000)msecs (0/0), process = Virtual Exec.
```


The workaround is to configure storm control on a port channel interface.
- CSCti78365
The config.text.backup file is present after the switch is restored to the factory defaults. There is no workaround.
- CSCti95834
When you enter the **ipv6 traffic-filter** interface configuration command, it might not filter traffic as expected, and it might allow traffic to pass through. There is no workaround.
- CSCti95979 (Catalyst 3750-X and 3750-E)
QoS ACL commands might appear differently in the running configuration after the master switch is reloaded or removed from the stack. The functionality of the commands remains the same. There is no workaround.

- CSCtj25488 (Catalyst 3750-X and 3750-E)

Two stacks that have members with fiber SFP modules are connected in a cross-stack EtherChannel with this configuration:

- Layer 3 EtherChannels
- EtherChannel **on** mode

If a member in one stack is reloaded, this error message appears on a member switch port in the other stack and the port is error disabled.

```
%PLATFORM_PM-3-INTVLANINUSE: internal vlan-id 1012 allocated for interface Gi2/0/2 is still in use (3750-b-2)-Traceback= 173E7F0 198F40C 176DA04 1774E70 173FBDC 1744574 16C9C28 17C65C4 17C67D8 1BB7308 1BADD78 (3750-b-2)
```

The workaround is to configure Layer 2 EtherChannels with SVIs and to use the EtherChannel **Active** mode.

- CSCtj03875

When you disconnect the spanning tree protocol (STP) peer link, the STP port path cost configuration changes.

There is no workaround.

- CSCtj75471

When a spanning-tree bridge protocol data unit (BPDU) is received on an 802.1Q trunk port and has a VLAN ID is greater than or equal to 4095, the spanning-tree lookup process fails.

There is no workaround.

- CSCtj88040 (Catalyst 3750-X and 3750-E)

When a stack is running per-VLAN spanning-tree plus (PVST+) and you create a VLAN, the STP topology change resets the aging time for all members and ages out all the MAC addresses for the new VLAN. If a cookie for the new VLAN on the member is not created when the master sends the member an HRPC message to update the aging timer, the member changes the aging time for VLAN 1 to that set during the topology change.

After the topology change, the aging time for the new VLAN is reset to that before the STP topology changed. However, the aging time for VLAN 1 does not change. The MAC addresses learned on VLAN 1 and on the member switch ports age out before aging time for the new VLAN.

The workaround is to disable STP before creating a new VLAN in the stack.

- CSCtj88307

When you enter the **default interface**, **switchport**, or **no switchport** interface configuration command on the switch, this message appears: *EMAC phy access error, port 0, retrying.....*

There is no workaround.

- CSCtj95182

When you use a network scanner to check network devices for security issues, the CPU usage increases.

There is no workaround.

- CSCtk11275

On a switch running Cisco IOS Release 12.2(55)SE with the **parser config cache interface** global configuration command in the configuration, when you use the CISCO-MAC-NOTIFICATION-MIB to enable the SNMP MAC address notification trap, the trap is enabled, but the trap setting does not appear in the switch configuration.

The workaround is to remove the **parser config cache interface** command from the configuration.

- CSCtk13113

The CPU usage on a standalone switch varies as the switch updates the running configuration.

There is no workaround.

- CSCtk32638 (Catalyst 3750-X and 3750-E)

When the switch stack elects a new stack master, by default the MAC address of the new master becomes the stack MAC address. Configuring a persistent MAC address sets a delay after stack master change before the stack master MAC address change. A timer value of 0 means that the MAC address of the current master is used indefinitely.

When you enter the **stack-mac persistent timer 0** global configuration command on a stack and the master switch is not the original owner of the stack MAC address, ports on member switches do not go through Rapid Spanning Tree Protocol (STP) transitions directly into the forwarding state.

The workaround is to not use the **stack-mac persistent timer 0** command on the switch stack.

- CSCtk54457 (Catalyst 3750-X and 3560-X)

On Catalyst 2960-S, 3560-X, and 3750-X switches, some SFP+ module ports do not work correctly with 1 Gigabit SFP modules when the speed for the port and for the connected device is set to **nonegotiate**. This occurs only on some ports and some SKUs.

The workaround is to set the speed on the SFP interface to autonegotiate by entering the **speed auto** interface configuration command.

- CSCtl11469 (PoE switches)

The SNMP Get action does not work correctly on Cisco IOS Releases 12.2(46)SE and 12.2(53)SE with the pethMainPseOperStatus operation.

The workaround is to use the SNMP Walk utility instead of SNMP Get.

- CSCtl42740

When 802.1x MAC authentication bypass with multidomain authentication and critical VLAN are enabled on an interface on a switch running Cisco IOS Release 12.2(53)SE or later, if the switch loses connectivity with the AAA server, the switch might experience high CPU usage and show these messages:

```
AUTH-EVENT (Gi0/15) Received clear security violation
AUTH-EVENT (Gi0/15) dot1x_is_mab_interested_in_mac: Still waiting for a MAC on port
GigabitEthernet0/15
```

There is no workaround.

- CSCtl80678

The port manager callback might cause more than 90% CPU usage for up to 20 minutes under these conditions:

- Link comes up simultaneously on multiple dot1q trunk ports.
- VLAN Trunking Protocol (VTP) pruning is enabled.

The workaround is to disable VTP pruning.

- CSCto62631

A switch running Cisco IOS Release 12.2(58)SE might reload if:

- SSH version 2 is configured on the switch, and
- a customized login banner was configured by using the **banner login message** global configuration command

Use one of these workarounds:

- Disable the login banner by entering the **no login banner** command.
- Disable SSH on the switch.
- Downgrade to a software version prior to Cisco IOS Release 12.2(58)SE.

- CSCtt70484 (Catalyst 3750-X)

If you upgrade the Cisco Catalyst 3750-X switch in Cisco StackPower mode from Release 12.2(58)SE, the switch may repeatedly report under-budgeted power messages. This issue is caused by a change in the minimum power budget values.

There is no workaround.

Documentation Updates



Note

The “Supported MIBs” appendix is no longer in the software configuration guide. To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: <http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

- [Control Plane Protection, page 41](#)
- [Update to the Catalyst 3750-X and 3750-E Software Configuration Guides, page 42](#)
- [Updates to the Catalyst 3750-E and 3560-E Cisco Software Activation and Compatibility Document, page 42](#)
- [Updates to the System Message Guide, page 43](#)
- [Update to the Installation Notes for Catalyst 3750-X and 3560-X Switch Power Supply Modules, page 47](#)

Control Plane Protection

Catalyst 3750-X, 3750-E, 3560-X and 3560-E switches internally support up to 16 different control plane queues. Each queue is dedicated to handling specific protocol packets and is assigned a priority level. For example, STP, routed, and logged packets are sent to three different control plane queues, which are prioritized in corresponding order, with STP having the highest priority. Each queue is allocated a certain amount of processing time based on its priority. The processing-time ratio between low-level functions and high-level functions is allocated as 1-to-2. Therefore, the control plane logic dynamically adjusts the CPU utilization to handle high-level management functions as well as punted traffic (up to the maximum CPU processing capacity). Basic control plane functions, such as the CLI, are not overwhelmed by functions such logging or forwarding of packets.

Update to the Catalyst 3750-X and 3750-E Software Configuration Guides

Correction to the “Unsupported Commands in Cisco IOS Release 12.2(58)SE” Chapter

The “Miscellaneous Unsupported Privileged EXEC Commands” section should include the **show facility-alarm status** privileged EXEC command for the Catalyst 3750-E switch.

Update to the “Managing Switch Stacks” Chapter

In the “Managing Switch Stacks” chapter, this information is added.

In a mixed stack that has Catalyst 3750-X, Catalyst 3750-E, and Catalyst 3750 switches, we recommend that a Catalyst 3750-X switch be the master and that all stack members run Cisco IOS Release 12.2(53)SE2 or later. The Catalyst 3750 image is on the Catalyst 3750-X and 3750-E switches to simplify switch management.

To upgrade the stack, use the **archive download-sw** privileged EXEC command to download images to the master. For example, use the **archive download-sw /directory tftp://10.1.1.10/c3750-ipservicesk9-tar.122-55.SE1.tar c3750e-universalk9-tar.122-55.SE1.tar** command to specify a directory, following the command with the list of tar files to download for the members.

- The c3750-ipservicesk9-tar.122-55.SE1.tar is for the Catalyst 3750 members.
- The c3750e-universalk9-tar.122-55.SE1.tar is for the Catalyst 3750-X and 3750-E members.

You can display the file list that is in the flash memory:

```
Switch# dir flash: c3750e-universalk9-tar.122-55.SE1
Directory of flash:/c3750e-universalk9-tar.122-55.SE1/

 5  -rwx   14313645   Mar 1 1993 00:13:55 +00:00  C3750e-universalk9-tar.122-55.SE1.tar
 6   drwx    5632     Mar 1 1993 00:15:22 +00:00  html
443 -rwx    444      Mar 1 1993 00:15:58 +00:00  info
444 -rwx   14643200   Mar 1 1993 00:04:32 +00:00  c3750-ipservicesk9-tar.122-55.SE1.tar
```

Updates to the Catalyst 3750-E and 3560-E Cisco Software Activation and Compatibility Document

In Cisco IOS Release 12.2(50)SE1 and earlier, the Catalyst 3750-E and 3560-E switches support only the universal software images.

- In Cisco IOS Release 12.2(50)SE2 or later, the Catalyst 3750-E and 3560-E switches support the universal and IP base software images. In the *Cisco Software Activation and Compatibility Document*:
- If your switch is running the universal software image, all the sections in the “Software Activation” section apply.
- If your switch is running the IP base image, only the “Displaying Software License Information” in the “Software Activation” section applies.

Updates to the System Message Guide

New System Messages

Error Message IP-3-SBINIT: Error initializing [chars] subblock data structure.
[chars]

Explanation The subblock data structure was not initialized. [chars] is the structure identifier.

Recommended Action No action is required.

Error Message VLMAPLOG-6-ARP: vlan [dec] (port [chars]) denied arp ip [inet] -> [inet], [dec] packet[chars]

Explanation A packet from the virtual LAN (VLAN) that matches the VLAN access-map (VLMAP) log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] denotes the number of packets, and the second [chars] represents the letter “s” to indicate more than one packet.

Recommended Action No action is required.

Error Message VLMAPLOG-6-L4: vlan [dec] (port [chars]) denied [chars] [inet]([dec]) -> [inet]([dec]), [dec] packet[chars]

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the second [chars] is the protocol, the first [inet] is the source IP address, the second [dec] is the source port, the second [inet] is the destination IP address, the third [dec] is the destination port, the fourth [dec] denotes the number of packets, and the third [chars] represents the letter “s” to indicate more than one packet.

Recommended Action No action is required.

Error Message VLMAPLOG-6-IGMP: vlan [dec] (port [chars]) denied igmp [inet] -> [inet]([dec]), [dec] packet[chars]

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] is the Internet Group Management Protocol (IGMP) message type, the third [dec] denotes the number of packets, and the second [chars] represents the letter “s” to indicate more than one packet.

Recommended Action No action is required.

Error Message VLMAPLOG-6-ICMP: vlan [dec] (port [chars]) denied icmp [inet] -> [inet] ([dec]/[dec]), [dec] packet[chars]

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] is the Internet Control Message Protocol (ICMP) message type, the third [dec] is the ICMP message code, the fourth [dec] denotes the number of packets, and the second [chars] represents the letter “s” to indicate more than one packet.

Recommended Action No action is required.

Error Message VLMAPLOG-6-IP: vlan [dec] (port [chars]) denied ip protocol=[dec] [inet] -> [inet], [dec] packet[chars]

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the second [dec] is the protocol number, the first [inet] is the source IP address, the second [inet] is the destination IP address, the third [dec] denotes the number of packets, and the second [chars] represents the letter “s” to indicate more than one packet.

Recommended Action No action is required.

Error Message HARDWARE-2-PSU_THERMAL_WARNING: PSU [chars] temperature has reached warning threshold

Explanation The switch power supply unit (PSU) temperature sensor value has reached the warning level. The external temperature is high. [chars] is the power supply.

Recommended Action Reduce the temperature in the room. (The switch functions normally until the temperature reaches the critical level.)

Error Message HARDWARE-1-PSU_THERMAL_CRITICAL: PSU [chars] temperature has reached critical threshold

Explanation The switch PSU temperature sensor value has reached the critical level, and the switch cannot function normally. The external temperature is very high. [chars] is the power supply.

Recommended Action Immediately reduce the room temperature.

Error Message HARDWARE-5-PSU_THERMAL_NORMAL: PSU [chars] Temperature is within the acceptable limit

Explanation The switch PSU temperature sensor value is within normal limits. [chars] is the power supply.

Recommended Action No action is required.

Error Message `HARDWARE-2-THERMAL_WARNING: Temperature has reached warning threshold`

Explanation The switch temperature sensor value has reached the warning level. The external temperature is high.

Recommended Action Reduce the room temperature. (The switch functions normally until the temperature reaches the critical level.)

Error Message `PLATFORM_STACKPOWER-6-RPS_CABLE: RPS cable [chars]`

Explanation The redundant power supply (RPS) cable connected to the switch was connected or disconnected.

Recommended Action No action is required.

Error Message `PLATFORM_STACKPOWER-6-RPS_LINK: RPS protocol is up`

Explanation The RPS can now provide backup power.

Recommended Action No action is required.

Error Message `PLATFORM_STACKPOWER-6-RPS_BACKUP: RPS backup is [chars]`

Explanation The status of the RPS backup for the switch. [chars] identifies the active or inactive status.

Recommended Action If the RPS backup is inactive, replace power supplies that are faulty or removed.

Error Message `PLATFORM_STACKPOWER-6-SW_RPS_CABLE: Switch [dec] RPS cable [chars]`

Explanation The RPS cable connected to the switch was connected or disconnected.

Recommended Action No action is required.

Error Message `PLATFORM_STACKPOWER-6-SW_RPS_LINK: Switch [dec] RPS protocol is up`

Explanation The RPS can now provide backup power.

Recommended Action No action is required

Error Message `PLATFORM_STACKPOWER-6-SW_RPS_BACKUP: Switch [dec] RPS backup is [chars]`

Explanation The status of the RPS backup for the switch. [dec] is the switch identifier, and [chars] identifies the active or inactive status.

Recommended Action If the RPS is inactive, replace power supplies that are faulty or have been removed.

Error Message PLATFORM_STACKPOWER-6-TOO_MANY_ERRORS: Switch [dec]: Too many errors seen on port [chars]

Explanation Several errors have occurred on the switch stack power port. [chars] is the port.

Recommended Action Check the power supplies and cables connected to the port. Contact your Cisco sales representative for assistance.

Error Message AUTHMGR-7-STOPPING: Stopping '[chars]' for client [enet] on Interface [chars] AuditSessionID [chars]

Explanation The authentication process has been stopped. The first [chars] is the authentication method, [enet] is the Ethernet address of the host, the second [chars] is the interface for the host, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation All available authentication methods have been tried. The first [chars] is the client identifier, the second [chars] is the interface for the client, and the third [chars] is the session ID.

Recommended Action No action is required.

Modified System Messages

Error Message ILPOWER-5-ILPOWER_POWER_DENY: Interface [chars]: inline power denied

Explanation The switch does not have enough power to supply the Power over Ethernet (PoE) port. [chars] is the PoE port identifier.

Recommended Action No action is required.

Error Message AUTHMGR-5-MACMOVE: MAC address ([enet]) moved from Interface [chars] to Interface [chars]

Explanation The client moved to a new interface but did not log off from the first interface. [enet] is the MAC address of the client, the first [chars] is the earlier interface, and the second [chars] is the newer interface.

Recommended Action No action is required.

Error Message AUTHMGR-5-MACREPLACE: MAC address ([enet]) on Interface [chars] is replaced by MAC ([enet])

Explanation A new client has triggered a violation that caused an existing client to be replaced. The first [enet] is the first client, [chars] is the interface, the second [enet] is the new client.

Recommended Action No action is required.

Error Message MAB-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation Authentication was unsuccessful. The first [chars] is the client, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message MAB-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation Authentication was successful. The first [chars] is the client, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Deleted System Messages

Error Message IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry: [inet], hw: [enet] by hw: [enet]\n", MSGDEF_LIMIT_FAST

Explanation Multiple stations are configured with the same IP address in a private VLAN. (This could be a case of IP address theft.) [inet] is the IP address that is configured, the first [enet] is the original MAC address associated with the IP address, and the second [enet] is the MAC address that triggered this message.

Recommended Action Change the IP address of one of the two systems.

Update to the Installation Notes for Catalyst 3750-X and 3560-X Switch Power Supply Modules

Installation Guidelines Change

The power supply is hot-swappable. In some configurations, such as full POE+ or power sharing mode, removing a power supply causes the switch to shut down powered devices until the power budget matches the input power of a single power supply. To minimize network interruption, hot swap the power supply under these circumstances:

- The switch is connected to an XPS-2200 and sufficient power is available.
- The switch is in StackPower mode and sufficient power is available (Catalyst 3750-X only).
- The switch is powered by other switches in a power stack, and no active backup is in progress.

Update to the Catalyst 3750-E and 3560-E Getting Started Guides

The warranty section in the *Catalyst 3750-E Switch Getting Started Guide* and the *Catalyst 3560-E Switch Getting Started Guide* has changed. These are the updated sections.

Catalyst 3750-E Switch Getting Started Guide

Catalyst 3750-E switches are covered by the Cisco Limited Lifetime Hardware Warranty. For more information, see this document on Cisco.com:

http://www.cisco.com/en/US/docs/general/warranty/English/LH2DEN__.html



Note

If you purchased your Catalyst 3750-E switch before May 1, 2009, your switch is covered by the Cisco 90-Day Limited Hardware Warranty. For more information, see this document on Cisco.com:

http://www.cisco.com/en/US/docs/general/warranty/English/901DEN__.html

Catalyst 3560-E Switch Getting Started Guide

Catalyst 3560-E switches are covered by the Cisco Limited Lifetime Hardware Warranty. For more information, see this document on Cisco.com:

http://www.cisco.com/en/US/docs/general/warranty/English/LH2DEN__.html



Note

If you purchased your Catalyst 3560-E switch before May 1, 2009, your switch is covered by the Cisco 90-Day Limited Hardware Warranty. For more information, see this document on Cisco.com:

http://www.cisco.com/en/US/docs/general/warranty/English/901DEN__.html

Related Documentation

User documentation in HTML format includes the latest documentation updates and might be more current than the complete book PDF available on Cisco.com.

with complete information about the switch are available from these Cisco.com sites:

Catalyst 3750-X

http://www.cisco.com/en/US/products/ps10745/tsd_products_support_series_home.html

Catalyst 3560-X

http://www.cisco.com/en/US/products/ps10744/tsd_products_support_series_home.html

Catalyst 3750-E

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

Catalyst 3560-E

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

These documents provide complete information about the switches:

- *Release Notes for the Catalyst 3750-X, Catalyst 3750-E, Catalyst 3560-X, and 3560-E Switches*
- *Catalyst 3750-X and 3560-X Switch Software Configuration Guide*
- *Catalyst 3750-X and 3560-X Switch Command Reference*

- *Catalyst 3750-X, 3750-E, 3560-X, and 3560-E Switch System Message Guide*
- *Cisco IOS Software Installation Document.*
- *Catalyst 3750-X and 3560-X Switch Getting Started Guide*
- *Catalyst 3750-X and 3560-X Switch Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 3750-X and 3560-X Switch*
- *Installation Notes for the Catalyst 3750-X and 3560-X Switch Power Supply Modules*
- *Installation Notes for the Catalyst 3750-X and 3560-X Switch Fan Module*
- *Installation Notes for the Catalyst 3750-X and 3560-X Switch Network Modules*
- *Catalyst 3750-E and Catalyst 3560-E Switch Software Configuration Guide*
- *Catalyst 3750-E and Catalyst 3560-E Switch Command Reference*
- *Cisco Software Activation and Compatibility Document*
- *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*
- *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*
- *Cisco eXpandable Power System 2200 Hardware Installation Guide*
- *Configuring the Cisco eXpandable Power System (XPS) 2200*
- *Auto Smartports Configuration Guide*
- *Cisco EnergyWise Configuration Guide*
- *Smart Install 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
- 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*

These documents have information about the Cisco enhanced EtherSwitch service modules:

- *Connecting Cisco Enhanced EtherSwitch Service Modules to the Network:*
http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/eesm_hw.html
- *Cisco Enhanced EtherSwitch Service Modules Configuration Guide:*
http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/eesm_sw.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:

<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 “[Obtaining Documentation and Submitting a Service Request](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2011–2012 Cisco Systems, Inc. All rights reserved.