Release Notes for Catalyst 3750-X, 3750-E, 3560-X, and 3560-E Switches, Cisco IOS Release 15.0(1)SE and Later

Revised June 29, 2012

Cisco IOS Release 15.0(1)SE 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 11 and the "Related Documentation" section on page 62.

These release notes include important information about Cisco IOS Release 15.0(1)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 10.
- 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 11.

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

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

© 2012 Cisco Systems, Inc. All rights reserved.

Contents

System Requirements

Supported Hardware

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

Switch Model	Description	Supported by Minimum Cisco IOS Release
Catalyst 3560X-24T-E	24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; IP Services feature set	12.2(53)SE2
Catalyst 3560X-48T-E	48 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; IP Services feature set	12.2(53)SE2
Catalyst 3560X-24P-E	24 10/100/1000 PoE+ [2] ports, 1 network module slot, 715 W power supply; IP Services feature set	12.2(53)SE2
Catalyst 3560X-48P-E	48 10/100/1000 PoE+ [2] ports, 1 network module slot, 715 W power supply; IP Services feature set	12.2(53)SE2
Catalyst 3560X-48PF-E	48 10/100/1000 PoE+[2] ports, 1 network module slot, 1100 W power supply; IP Services feature set	12.2(53)SE2
Catalyst 3750X-24T-E	24 10/100/1000 Ethernet ports, StackWise Plus, StackPower, 1 network module slot, 350 W power supply; IP Services feature set	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
Catalyst 3750X-48T-E	48 10/100/1000 Ethernet ports, StackWise Plus, StackPower, 1 network module slot, 350 W power supply; IP Services feature set	12.2(53)SE2
Catalyst 3750X-24P-E	24 10/100/1000 PoE+[2] ports, StackWise Plus, StackPower, 1 network module slot, 715 W power supply; IP Services feature se	12.2(53)SE2
Catalyst 3750X-48P-E	48 10/100/1000 PoE+ [2] ports, StackWise Plus, StackPower, 1 network module slot, 715 W power supply; IP Services feature set	12.2(53)SE2
Catalyst 3750X-48PF-E	48 10/100/1000 PoE+[2] ports, StackWise Plus, StackPower, 1 network module slot, 1100 W power supply; IP Services feature set	12.2(53)SE2
Catalyst 3750-X-12S-S	12 SFP module slots, StackWise Plus, StackPower, 1 network module slot, 350-W power supply; IP Base feature set	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	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	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	12.2(58)SE1
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	12.2(53)SE2
Catalyst 3750-X-48T-L	48 10/100/1000 Ethernet ports, StackWise Plus, 1 network module slot, 350 W power supply; LAN Base feature set	12.2(53)SE2
Catalyst 3750-X-24P-L	24 10/100/1000 PoE+[1] ports, StackWise Plus, 1 network module slot, 715 W power supply; LAN Base feature set	12.2(53)SE2
Catalyst 3750-X-48P-L	48 10/100/1000 PoE+[2] ports, StackWise Plus, 1 network module slot, 715 W power supply; LAN Base feature set	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	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	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	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	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	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]	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
Catalyst 3560-X-24T-L	24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; LAN Base feature set	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	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	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	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	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	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	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	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	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	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[2] DWDM[3] **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	12.2(53)SE2
SFP+ Modules	SFP-10G-SR SFP-10G-LR SFP-10G-LRM SFP-H10GB CU1M SFP-H10GB CU3M SFP-H10GB CU5M	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
Support for these SFP+ modules	Only version 02 (or later) of the CX1[4] cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	12.2(53)SE2
SFP module patch cable[5]	CAB-SFP-50CM	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.	12.2(53)SE2
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.	12.2(53)SE2
C3KX-NM-1G 1-Gigabit Ethernet Network Module	Four 1-Gigabit SFP module slots.	12.2(53)SE2
C3KX-NM-10GT 10-Gigabit Ethernet Network Module	Two 10-Gigabit Ethernet (copper) ports. **Note** To configure the port speed to 1 Gigabit per second, use the **hw-module switch** global configuration command.	15.0(1)SE
C3KX-SM-10G 10-Gigabit Ethernet Network Services Module	Two SFP+ module slots. The services module supports Net Flow and MACSec Uplink Encryption (switch- to-switch encryption between uplinks).	15.0(1)SE
eXpandable power system (XPS)	Cisco XPS 2200	12.2(55)SE1

1. PoE+ = Power over Ethernet, up to 30 W per port
2. CWDM = coarse wavelength-division multiplexer
3. DWDM = dense wavelength-division multiplexer
4. The CX1 cables are used with the OneX converters.
5. 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
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

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
SFP modules	1000BASE-LX/LH 1000BASE-SX 1000BASE-ZX 1000BASE-BX10-D 1000BASE-BX10-U 1000BASE-T 100BASE-FX	Cisco IOS Release 12.2(35)SE2
	CWDM[3]SFP-10G-SR SFP-10G-LR	Cisco IOS Release 12.2(53)SE
	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	

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
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
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

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
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

1. PoE = Power over Ethernet.
2. SFP = small form-factor pluggable
3. CWDM = coarse wavelength-division multiplexer
4. DOM = digital optical monitoring
5. Only Catalyst 3560-E switches. The SFP module patch cable is a 0.5-meter, copper, passive cable with SFP module connectors at each end. The patch cable can connect two Catalyst 3560-E switches in a cascaded configuration.
6. The CX1 cables are used with the OneX converter and are supported in Cisco IOS Release 12.2(53)SE and later.
7. 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 or 7.0, and Firefox up to version 27, 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 15.0(1)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/pcgi-bin/tablebuild.pl/NetworkAssistant

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

Upgrading the Switch Software

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.150-1.SE.tar c3560e-ipbasek9npe-tar.150-1.SE.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

Table 4 Software Images (continued)

Image	Filename	Description
IP base with payload encryption	c3750e-ipbasek9-tar.150-1.SE.tar c3560e-ipbasek9-tar.150-1.SE.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.150-1.SE.tar c3560e-universalk9npe-tar.150-1.SE.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.150-1.SE.tar c3560e-universalk9-tar.150-1.SE.tar	All the supported universal image features, Kerberos, SSH, SSL, SNMPv3, and MACsec LAN base, IP base, and IP services software licenses
Network services module software	c3kx-SM10G-tar.150-1.SE.tar	Supports service-module-specific features. Image must be compatible with the IOS image. See the "Catalyst 3750-X and 3560-X Network Services Module Software" section on page 14.
Catalyst 3750-E and Catalyst 3560-E switches		
IP base image	c3750e-ipbasek9-tar.150-1.SE.tar c3560e-ipbasek9-tar.150-1.SE.tar	Layer 2 and basic Layer 3 features, SSH, SSL, SNMPv3, and Kerberos
Universal image	c3750e-universalk9-tar.150-1.SE.tar c3560e-universalk9-tar.150-1.SE.tar	All the supported universal image features, Kerberos, SSH, SSL, and SNMPv3 IP base and IP services software licenses
Cisco enhanced EtherSwitch service modules		
LAN base image	c2960-lanbasek9-tar.150-1.SE.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.150-1.SE.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 11 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/web/download/index.html

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

c. Navigate to your switch model.

d. Click **IOS Software**, and 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.

Catalyst 3750-X and 3560-X Network Services Module Software

The network services module requires an additional software image to support the features that are available only on the service module. You use the **archive download-sw** privileged EXEC command on the switch to download the software image, which must be compatible with the Cisco IOS software running on the switch. If the versions are not compatible, the service module runs in pass-through mode, which means that none of the service-module-specific features are available.

When you install a network services module and boot up the switch, the switch runs a compatibility check to verify that the software version in the service module is compatible with the software running on the switch.

When you download software by entering the **archive download-sw** privileged EXEC command, the switch also runs a version check to verify software compatibility, if applicable:

- If the switch is in a switch stack, it checks the compatibility of the stack protocol and the switches in the stack.

- If a network services module is installed, it checks the compatibility of the switch software and the network services module software.

Note If the switch is not in a stack or if there is no network services module installed, no version compatibility check is needed.

If a mismatch between the service module and the switch is detected, this syslog message appears:

```
The FRULink 10G Service Module (C3KX-SM-10G) software version
is incompatible with the IOS software version. Please update
the software. Module is in pass-thru mode.
```

Service-module-specific features require the IP base or IP services feature set. If the switch is running the LAN base software feature set, this message appears:

```
Mar  1 00:01:32.341: %PLATFORM_SM10G-6-LICENSE: FRULink 10G Service Module
(C3KX-SM-10G) features are not supported with this license level. Module is in
pass-thru mode.
```

You can use the **show switch service-module** user EXEC command to view a service module on the switch or any service modules in the stack, and the service module software version supported by the switch/

This is an example of output when the software versions are compatible:

```
Switch# show switch service-modules
Switch/Stack supports service module CPU version: 03.00.24
                          Temperature                    CPU
Switch#  H/W Status       (CPU/FPGA)      CPU Link      Version
----------------------------------------------------------------
1       OK               86C/70C         connected     03.00.24
```

This is an example of output when a switch with a service module installed is running the LAN base feature set:

```
Switch# show switch service-modules
Switch/Stack supports service module CPU version: 03.00.25
                          Temperature                    CPU
Switch#  H/W Status       (CPU/FPGA)      CPU Link      Version
----------------------------------------------------------------
1       LB-PASS-THRU *   71C/59C         notconnected  N/A

*   Module services not supported on a Lanbase license
```

To download the network services module software:

Step 1 Go to this URL and log in:

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

Step 2 Navigate to Switches > LAN Switches - Access

Step 3 Navigate to the Catalyst 3750-X or 3560-X switch page.

Step 4 Click IOS Software, and select the latest network services module release.

The image name will be in this format: c3kx-SM10G-tar.150-1.SE.tar

Follow the steps in the "Upgrading a Switch by Using the CLI" section on page 13 to use the **archive download-sw** command and to download the software.

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

Note Cisco IOS Software Release 15.0(1)SE on the Catalyst 3750-X and 3560-X switches has been submitted for certification under Federal Information Processing Standard Publication 140-2 (FIPS 140-2). FIPS 140-2 is a cryptographic-focused certification, required by many government and enterprise customers, which ensures the compliance of the encryption/decryption operations performed by the switch to the approved FIPS cryptographic strengths and management methods for safeguarding these operations.

- Support for critical voice VLAN to so that when authentication is enabled and the access control server is not available, traffic from the host tagged with the voice VLAN is put into the configured voice VLAN for the port. (Not supported on the Catalyst 3750-X and 3560-X LAN base feature set)

  See the "Documentation Updates" section on page 45.

- The command 'ip tcp adjust-mss' is not supported on the 3750x/3560x/3750g/3560g/3750e/3560e platforms.
- Network Edge Access Topology (NEAT) enhancement to control access to the supplicant port during authentication. (Not supported on the Catalyst 3750-X and 3560-X LAN base feature set)

  See the "Documentation Updates" section on page 45

- SXP version 2, syslog messages, and SNMP support for Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (SxP). (Not supported on the Catalyst 3750-X and 3560-X LAN base feature set)

  For more information about Cisco TrustSec, see the " SGT Exchange Protocol over TCP (SXP)" chapter in the *Cisco TrustSec Switch Configuration Guide* at this URL: http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/sxp_config.html

- Auto Smartport features with improved device classification capabilities and accuracy, increased device visibility, and enhanced macro management. The device classifier is enabled by default, and can classify devices based on DHCP options.

  For more information, see the *Auto Smartports Configuration Guide* for this release.

- Flexible NetFlow to monitor user-defined flows, collect flow statistics, perform per-flow policing on uplink ports, and export the flow statistics to a collector device. (Supported only on the Catalyst 3750-X and 3560-X network services module running the IP base or IP services feature set)

- MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. (Supported on switch downlink ports or on uplink ports on the Catalyst 3750-X and 3560-X network services module running the IP base or IP services feature set)
- Device Sensor - Scalable network embedded sensor features for identification and classification of devices on the network.

  For more information on Device Sensor, see the *Device Sensor Guide* at this URL: http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/15.0_1_se/device_sensor/guide/sensor_guide.html

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 sand 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
Critical voice VLAN	15.0(1)SE	3750-E, 3560-E 3750-X, 3560-X
NEAT enhancement to control access to the supplicant port	15.0(1)SE	3750-E, 3560-E 3750-X, 3560-X
Cisco TrustSec SXP version 2, syslog messages, and SNMP support	15.0(1)SE	3750-E, 3560-E 3750-X, 3560-X
Auto Smartports improved device classification	15.0(1)SE	3750-E, 3560-E 3750-X, 3560-X
Device Sensor	15.0(1)SE	3750-E, 3560-E 3750-X, 3560-X
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

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
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
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

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
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
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

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
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
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

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
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
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

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
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

- 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)

- Identity Services Engine (ISE) is not available on Catalyst 2000 series switches.
- The **device-sensor accounting** global configuration command is not available on Catalyst 2000 series switches.

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)

Spanning Tree Protocol

- 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.

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

- 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 it 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:

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

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

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

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

Hardware Limitations

C3KX-SM-10G Network Module (Catalyst 3750-X and 3560-X only)

NetFlow Data Export (NDE) fails when the IP address specified by the destination keyword belongs to a network that is connected to the Ethernet management port (FastEthernet0) on the switch.

There is no workaround. (CSCtt05810)

Important Notes

- "Switch Stack Notes" section on page 33
- "Control Plane Protection" section on page 33
- "Control Plane Protection" section on page 33
- "Device Manager Notes" section on page 34

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 and later are compatible with Catalyst 3750 switches and Cisco EtherSwitch service modules running Cisco IOS Release 12.2(35)SE and later. 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.

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.

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. • **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.

- 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.

- CSCtn46265 (Catalyst 3560-X and 3750-X

  When you enter the **copy running-config startup config** privileged EXEC command on the switch, the running configuration is not always saved to the startup configuration on the first attempt.

  There is no workaround. If you wait for a few minutes, the configuration is saved when the switch attempts it again.

- CSCtq35006

  On a switch stack, when an IP phone connected to a member switch has its MAC address authorized using the critical voice VLAN feature, if a master changeover occurs, the voice traffic is dropped. Drop entries for the IP phone appear in the MAC address table management (MATM) table. This occurs because the switch initially drops the voice traffic before reauthenticating critical voice VLAN traffic. The dropped entries are removed when critical voice VLAN authentication occurs.

  There is no workaround. The dropped entries are removed when the IP phone is reauthenticated.

- CSCtq38500

  When you configure port-based QoS with an ACL by using the ACL range option, problems can occur if you have also configured **mls qos trus**t on the interface.

  The workaround is to match traffic by using the single port equal (**eq**) option or to not configure **mls qos trust** on the interface.

- CSCtq39377

Port security violations might be ignored when Auto Smartports is enabled and a Smartport macro is applied to a secure port. This behavior occurs because IOS sensor (part of Auto Smartports) sets the host mode to multiple-authentication (multi-host mode) and enables 802.1x in the host access table. In multi-host mode, if the same MAC address in the same VLAN is seen on another port, then it is not allowed. Therefore the packet does not reach port-security module to create the violation.

The workaround is to enter the **no macro auto monitor** global configuration command to globally disable the IOS sensor (Auto Smartports) feature.

- CSCtq76989 (Catalyst 3750-X or 3560-X switches)

  A *seed* switch is connected to a RADIUS server either directly or through a trunk port. A *non-seed switch* authenticates with the RADIUS server through the *seed* switch, based on the credential information defined in the RADIUS server. Cisco TrustSec (CTS) parameters must be configured on both the *seed* switch and the *non-seed* switch trunk interfaces.

  Although the *non-seed* switch is authenticated and authorized to connect to the network, supplicant devices connected to the *non-seed* switch might be unable to connect to the network, under these circumstances:

  – CTS caching is enabled on the *seed* switch and not enabled on the *non-seed* switch.

  – The *seed* switch reported the 802.1x role of the *non-seed* switch CTS trunk as authenticator in multi-host mode.

  – The *non-seed* switch reported this CTS trunk as the 802.1x authenticator role in single host mode and as supplicant.

  The workaround is to reduce the reauthentication time on the *seed* switch, or enter the **shutdown** interface configuration command, followed by the **no shutdown** interface configuration command on the *seed* switch CTS trunk interface.

- CSCtq81500

  When an IP phone is authenticated on a switch port that is running Multidomain authentication (MDA) in the voice VLAN, the switch might experience high CPU usage after continued attempts to re-authenticate a phone that does not have a valid password configuration. Re-authentication can be triggered by:

  – Expiration of the authentication timer

  – Entering the **dot1x re-authenticate interface** *interface-id* privileged EXEC command

  The workaround to clear the problem:

  – Enter the **shutdown** interface command followed by the **no shutdown** interface configuration command.

  – Initialize the interface by entering the **dot1x initialize interface** *interface-id* privileged EXEC command.

  – Correct the password on the phone.

  To prevent the situation:

  – Do not use periodic re-authentication for the voice domain.

  – When manually clearing authentications, use the **clear authentication session** privileged EXEC command instead of the **dot1x re-authenticate interface** command.

- CSCtr07908

  The image archive download process does not work if there is an *update* directory in flash memory, which occurs if a previous download was interrupted or failed.

The workaround is to delete the update directory from the flash memory before executing the **archive download-sw** privileged EXEC command.

- CSCtr16643

  When TCP packets in the same VLAN are sent from one switch to another, ACL deny logs appear, even though the ACL is applied on the switch virtual interface (SVI).

  The workaround, to stop the messages, is to configure IP unreachables by entering the **ip unreachables** interface configuration command on the SVI or routed port.

- CSCtr87645

  ASP now uses a device classifier, which determines the type of device that is connected to the switch. As a result, ASP has no control over the protocol type that is used to detect the device. Therefore, the protocol detection controls are deprecated. When you enter the **macro auto global control detection** command, the protocol does not show up in the running configuration; however, the **filter-spec** command is shown in the output.

  There is no workaround. To see the deprecated commands, enter the **show running config deprecated** global and interface configuration command.

- CSCtt11621

  When the **dot1x default** interface configuration command is entered, access control for hosts is disabled and the values for the following commands are reset to their default values: **authentication host-mode**, **authentication timer reauthenticate**, and **authentication port-control.**

  The workaround is to avoid using the **dot1x default** command and reset the 802.1x port parameters individually. Another workaround is to enter the **dot1x default** command, and then reconfigure the incorrectly changed values.

- CSCtt14788 (Catalyst 3560-X and 3750-X)

  NetFlow Data Export (NDE) packets might be dropped when virtual routing and forwarding (VRF) is configured on the switch and the exported traffic has conflicting information from the VRF tables and the routing information base.

  There is no workaround.

- CSCtt22566 (Catalyst 3560-X and 3750-X)

  Monitored SPAN traffic is not sent to the SPAN destination when TrustSec MACsec is enabled on the SPAN source interface.

  There is no workaround.

- CSCtw33903

  This problem occurs when the Enterprise Policy Manager (EPM) for a device connected to an interface is authorized in closed mode and no policies are configured or downloaded. If no port ACL is configured, the auth-default access control list (ACL) is applied to the switch. If another device is connected to this device, restricted VLAN (authentication event interface configuration command) is enabled on the port. The Application Control Engine (ACE) is not configured to permit traffic originating from the connected device, and IP packets are dropped.

  The workaround is to configure a port ACL to allow IP traffic for the specific IP range for the connected devices on the interface.

- CSCtw42349

  This problem occurs when a supplicant device is connected to a switch through a main device, and the interface is enabled with authentication, port security and IP source guard (IPSG). The main and supplicant devices are configured with sticky MAC addresses. In this case, if the port is shut down, traffic originating from the supplicant is dropped.

The workaround is to disable port security on the port.

- 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.

- CSCue23882

  If a new port is added to an etherchannel on a switch using DAI or IPDT, ARP packets that ingress the port are lost.

  The workaround is to save the configuration and reload the switch. Alternatively, configure the switch by entering the no macro auto monitor command followed by the macro auto monitor command after the port is bundled for the first time.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.0(1)SE3

- CSCtj48387

  A router running as a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) halts with DHCP-related errors. This problem occurs when DHCP is enabled and sessions receive DHCP information from a RADIUS server.

  There is no workaround.

- CSCtl60151

  The switch might occasionally reload after experiencing a CPU overload, regardless of what process is overloading the CPU.

  There is no workaround.

- CSCtn11683 (Catalyst Switches 3560-X and 3750-X)

  A Catalyst 3560-X or 3750-X switch port might stop forwarding traffic. The packet counters increment for sent packets, but not for received packets.

  The workaround, to bring up the port, is to save the configuration and to restart the switch.

- CSCts50508

  When authentication is enabled on an open port (for example, when moving from no authentication to authentication port-control auto), Address Resolution Protocol (ARP) and DHCP traffic is dropped.

The workaround is to use the **shutdown** configuration interface command to disable the port and then use the **no shutdown** configuration interface command to enable the port. You also can use the **clear mac-address-table** command to clear the MAC address table.

- CSCts74537

  After reloading the switch, Switched Port Analyzer (SPAN) traffic does not arrive at the SPAN destination port.

  The workaround is to delete the SPAN configuration and reapply it.

- CSCtt04584

  On a virtual routing and forwarding (VRF) interface, IP multicast traffic is not forwarded after using the **clear ip mroute vrf** command.

  There is no workaround.

- CSCtu08022 (Catalyst Switch 3750-X Models WS-3750X-12-S and WS-3750X-24-S)

  When duplex mode is configured on the downlink ports of a Catalyst WS-3750X-12-S or a Catalyst WS-3750X-24-S stacked switch, the downlink interfaces revert to auto-negotiate mode when the stack is restarted. This issue does not affect ports on the stack master, but affects all slave switches of type C3750X-12S and C3750X-24S.

  The workaround is to use no more than one WS-3750X-12-S or WS-3750X-24-S switch on a stack and to specify that switch as the stack master.

- CSCtu09817 (Catalyst Switches 3560-E and 3750-E)

  When a power supply fails or loses power, the redundant power supply (RPS) (750 W or 1150 W) does not provide Power over Ethernet (PoE) for the powered devices.

  There is no workaround.

- CSCtx05704 (Catalyst Switches 3750-E and 3750-X)

  After a rolling stack upgrade, Address Resolution Protocol (ARP) entries are in the INCOMPLETE state.

  There is no workaround.

- CSCtx47330 (Catalyst Switches 3750-E and 3750-X)

  After resetting a four-member stacked switch that includes a four-port Gigabit Ethernet network module, Gigabit Ethernet ports do not work.

  There is no workaround.

- CSCty07602 (Catalyst Switches 3560-X and 3750-X)

  The switch drops transient routed and switched IP UDP fragments while printing the following message on the console:

  `%PLATFORM_IPC-3-COMMON: Unknown IPC message type <type> size <size>`

  where *<type>* corresponds to the middle 2B of the frame destination MAC address in decimal format and *<size>* corresponds to size of a dropped packet.

  There is no workaround. To retain the functionality, downgrade to Cisco IOS Release 12.2(58)SE2.

- CSCty58433 (Catalyst Switches 3560-X and 3750-X)

  When many static Address Resolution Protocol (ARP) entries are created in a short period of time, the switch might unexpectedly reload.

  There is no workaround.

- CSCty96049

  Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

  Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcp

Caveats Resolved in Cisco IOS Release 15.0(1)SE2

- CSCtq22963 (Catalyst 3560-X and 3750-X)

  NetFlow traffic export fails when the source interface IP address and destination IP address are on different subnets.

  There is no workaround.

- CSCtw91517 (Catalyst Switches 3560-X and 3750-X)

  If network module C3KX-SM-10G is installed on Cisco IOS Release 15.0(1)SE1, the module does not boot properly and a version mismatch error is displayed.

  This problem is fixed in Cisco IOS Release 15.0(1)SE2.

Caveats Resolved in Cisco IOS Release 15.0(1)SE1

- CSCth62705

  CPU usage in the switch is high when you configure an EtherChannel and add new domain members or EnergyWise-capable endpoints with a different EnergyWise domain to an existing domain.

  The workaround is to disable the port channel where the high CPU usage is seen.

- CSCtq56690 - (Catalyst Switches 3750-X and 3560-X)

  If a switch contains two fan modules and you unplug one of the modules, the **snmpwalk** global configuration command does not show any output.

  There is no workaround.

- CSCtq75612

  If you combine two switches in a FlexStack configuration and set the password for the master switch, the change is not reflected in the **show run** command after you log out of the switch and log in again.

  There is no workaround

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCtr31957

  When the ipc_check_qtime_process() processes a message from the Inter-Process Communication (IPC) message table, it might be interrupted by the acknowledgement for that message. In this situation, the message becomes invalid because the interrupt handler returns that message to the message cache, and the switch crashes because it still attempts to access that message.

  There is no workaround.

- CSCtr49064

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

  The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

- CSCtr66767 - (Catalyst Switches 3750-X and 3560-X)

  On downlink ports that encrypt packet data between different switches, data is not encrypted for the following protocols: LLDP, LACP, PAUSE/MAC Ctl(0x8808), EAPOL, CDP, and all packets that use the same destination MAC address as CDP.

  There is no workaround to encrypt data for the SAP operation mode. We recommend that you use no encapsulation SAP operation mode by entering the **no-encap** interface configuration command.

- CSCtr75161

  When you configure a web authentication profile with an access control list (ACL) policy on a switch, and also configure port ACL, the port ACL is applied to a host when it falls back to the web ACL.

  There is no workaround. To retain the functionality, you can downgrade to Cisco IOS Release 12.2(55)SE.

- CSCtr75298 - (Catalyst Switches 3750-E, 3750-X and 3650-X

  A change of Authorization does not work on a switch that runs the LAN Base image.

  The workaround is to use the license for the IP Base image.

- CSCtr79386 - (Catalyst Switches 3750-E and 3750-X)

  When you enable Dynamic Host Configuration Protocol (DHCP) snooping, the incoming traffic exhausts the I/O memory and the switch crashes.

  The workaround is to disable DHCP snooping.

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

Cisco has released free software updates that address these vulnerabilities.

The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts07947 - (Catalyst Switches 3750-E and 3750-X)

  When you upgrade a stack of two switches using the Rolling Stack Upgrade (RSU) option, the connected switches reload simultaneously instead of sequentially. This problem happens because only one port of the active switch is disabled during the upgrade.

  The workaround to disable both stack ports has now been incorporated into the switch.

- CSCts36715

  When a client connection to the web server fails, with each subsequent attempt the HTTP proxy server process is stuck and a new HTTP proxy server is created. To see these processes, enter the **show processes** command. When the number of processes reach the limit specified in the **ip admission http proxy** interface configuration command, all subsequent web authentications fail.

  The workaround is to reload the switch.

- CSCts88664

  During local web authentication, the switch crashes and reboots if the user enters his or her credentials and logs in instantly.

  The workaround is to enter the user credentials and log in after a pause of 4-5 seconds.

- CSCtt16051

  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

- CSCtt18020

  The router reloads unexpectedly. This issue is seen when you log in to the router using SSH.

  The workaround is to log in to the router using Telnet.

- CSCtu09846

  The switch crashes when users are redirected using central web authentication.

  The workaround is to disable central web authentication.

Caveats Resolved in Cisco IOS Release 15.0(1)SE

- 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.

- 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

- CSCto10165

  A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available to mitigate this vulnerability other than disabling the Smart Install feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-smart-install.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.

Documentation Updates

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

Information Added to the "Administering the Switch" Chapter

In the section on "NTP Version 4," this information was added

You can disable NTP packets from being received on routed ports and VLAN interfaces. You cannot disable NTP packets from being received on access ports. For details, see the "Disabling NTPv4 Services on a Specific Interface" section of the "Implementing NTPv4 in IPv6" chapter of the *Cisco IOS IPv6 Configuration Guide, Release 12.4T.*

Correction to the "Managing Switch Stacks" Chapter

In the "Stack Master Election and Re-Election" section, the 20-second timeframe for participation in a stack master election is incorrect. The correct timeframe is 120 seconds.

The correct information appears in the online documentation:

http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3750x_3560x/software/release/15.0_1_se/configuration/guide/swstack.html#wp1228109

This correction does not appear in the full-book PDF of the software configuration guide.

Correction to the "Clustering Switches" Chapter

In the "Candidate Switch and Cluster Member Switch Characteristics" section, the requirements should include:

- The **ip http server** global configuration command must be configured on the switch.

Correction to the "Configuring STP" Chapter

In the "Displaying the Spanning-Tree Status" section of the "Configuring STP" chapter, this note should appear:

Note In a switch stack, the spanning-tree process reports both physical stack ports in a stack member as one logical port.

Correction to the "Unsupported Commands" Chapter

The "Miscellaneous" section should include the **logging discriminator** global configuration command.

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

Information Added to the “Configuring IEEE 802.1x Port-Based Authentication” Chapter

Configuring Critical Voice VLAN

When an IP phone connected to a port is authenticated by the access control server (ACS), the phone is put into the voice domain. If the ACS is not reachable, the switch cannot determine if the device is a voice device. If the server is unavailable, the phone cannot access the voice network and therefore cannot operate.

For data traffic, you can configure inaccessible authentication bypass, or critical authentication, to allow traffic to pass through on the native VLAN when the server is not available. If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network and puts the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. When the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated, the switch connects those hosts to critical ports. A new host trying to connect to the critical port is moved to a user-specified access VLAN, the critical VLAN, and granted limited authentication.

With this release, you can enter the **authentication event server dead action authorize voice** interface configuration command to configure the critical voice VLAN feature. When the ACS does not respond, the port goes into critical authentication mode. When traffic coming from the host is tagged with the voice VLAN, the connected device (the phone) is put in the configured voice VLAN for the port. The IP phones learn the voice VLAN identification through CDP (Cisco devices) or through LLDP or DHCP.

You can configure the voice VLAN for a port by entering the **switchport voice vlan**-*id* interface configuration command.

This feature is supported in multidomain and multi-auth host modes. Although you can enter the command when the switch in single-host or multi-host mode, the command has no effect unless the device changes to multidomain or multi-auth host mode.

Beginning in privileged EXEC mode, follow these steps to configure critical voice VLAN on a port and enable the inaccessible authentication bypass feature.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**radius-server dead-criteria time** *time* **tries** *tries*	Sets the conditions that are used to decide when a RADIUS server is considered unavailable or down (*dead*). • The range for *time* is from 1 to 120 seconds. The switch dynamically determines a default *seconds* value between 10 and 60 seconds. • The range for *tries* is from 1 to 100. The switch dynamically determines a default *tries* parameter between 10 and 100.
Step 3	**radius-server deadtime** *minutes*	(Optional) Sets the number of minutes during which a RADIUS server is not sent requests. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.

	Command	Purpose
Step 4	**radius-server host** *ip-address* [**acct-port** *udp-port*] [**auth-port** *udp-port*] [**test username** *name* [**idle-time** *time*] [**ignore-acct-port**] [**ignore-auth-port**]] [**key** *string*]	Configures the RADIUS server parameters: • **acct-port** *udp-port*—Specifies the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646. • **auth-port** *udp-port*—Specifies the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645. **Note** You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values. • **test username** *name*—Enables automatic testing of the RADIUS server status, and specifies the username to be used. • **idle-time** *time*—Sets the interval of time in minutes after which the switch sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour). • **ignore-acct-port**—Disables testing on the RADIUS-server accounting port. • **ignore-auth-port**—Disables testing on the RADIUS-server authentication port. • For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. You can also configure the authentication and encryption key by using the **radius-server key** {**0** *string* | **7** *string* | *string*} global configuration command.
Step 5	**interface** *interface-id*	Specifies the port to be configured and enters interface configuration mode.
Step 6	**authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*	Configures a critical VLAN to move hosts on the port if the RADIUS server is unreachable: • **authorize**—Moves any new hosts trying to authenticate to the user-specified critical VLAN. • **reinitialize**—Moves all authorized hosts on the port to the user-specified critical VLAN.
Step 7	**switchport voice vlan** *vlan-id*	Specifies the voice VLAN for the port. The voice VLAN cannot be the same as the critical data VLAN configured in Step 6.
Step 8	**authentication event server dead action authorize voice**	Configures critical voice VLAN to move data traffic on the port to the voice VLAN if the RADIUS server is unreachable.
Step 9	**end**	Returns to privileged EXEC mode.
Step 10	**show authentication interface** *interface-id*	(Optional) Verifies your entries.

This example shows how to configure the inaccessible authentication bypass feature and configure the critical voice VLAN:

```
Switch(config)# radius-server dead-criteria time 30 tries 20
Switch(config)# radius-server deadtime 60
Switch(config)# radius-server host 1.1.1.2 acct-port 1550 auth-port 1560 test username
user1 idle-time 30 key abc1234
Switch(config)# interface gigabitethernet 1/0/1
Switch(config)# radius-server deadtime 60
Switch(config-if)# authentication event server dead action reinitialicze vlan 20
Switch(config-if)# switchport voice vlan
Switch(config-if)# authentication event server dead action authorize voice
Switch(config-if)# end
```

Network Edge Access Topology (NEAT) Enhancement

NEAT can control traffic exiting the supplicant switch port during the authentication period. When you connect a supplicant switch to an authenticator switch that has BPDU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** global configuration command temporarily blocks the supplicant port during authentication to ensure that the authenticator port does not shut down before authentication completes. If authentication fails, the supplicant port opens. Entering the **no dot1x supplicant controlled transient** global configuration command opens the supplicant port during the authentication period. This is the default behavior.

We strongly recommend using the **dot1x supplicant controlled transient** command on a supplicant switch when BPDU guard is enabled on the authenticator switch port with the **spanning-tree bpduguard enable** cinterface configuration command.

Note If you globally enable BPDU guard on the authenticator switch by using the **spanning-tree portfast bpduguard default** global configuration command, entering the **dot1x supplicant controlled transient** command does not prevent the BPDU violation.

Information Added to the "Managing Switch Stacks" Chapter

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
```

Update to the Catalyst 3750-E and 3560-E Switch Software Configuration Guide

Correction to the "Configuring Network Security with ACLs" Chapter

There is an error in the "Creating a Numbered Extended ACL" section. Contrary to the note in this section, ICMP echo-replies can be filtered.

Updates to the Catalyst 3750-X and 3750-E Command Reference

These commands were added or revised:

- authentication event, page 49
- dot1x supplicant controlled transient, page 53

authentication event

To set the actions for specific authentication events on the port, use the **authentication event** interface configuration command. To return to the default settings, use the **no** form of the command.

authentication event {[**linksec**] **fail** [**retry** *retry count*] **action** {**authorize vlan** *vlan-id* | **next-method**}} | {**no-response action authorize vlan** *vlan-id*} | {**server** {**alive action reinitialize**} | {**dead action** {**authorize** {**vlan** *vlan-id* | **voice**} | **reinitialize vlan** *vlan-id*}}

no authentication event {[**linksec**] **fail** | **no-response** | {**server** {**alive**} | {**dead** [**action** {**authorize** {**vlan** *vlan-id* | **voice**} | **reinitialize vlan**}] }

Syntax Description

action	Configures the required action for an authentication event.
alive	Configures the authentication, authorization, and accounting (AAA) server alive actions.
authorize	Authorizes the VLAN on the port.
dead	Configures the AAA server dead actions.
fail	Configures the failed-authentication parameters.
linksec fail action	See the **authentication event linksec fail action** command. (Catalyst 3750-X and 3560-X only)
next-method	Moves to next authentication method.

no-response	Configures the nonresponsive host actions.
reinitialize	Reinitializes all authorized clients.
retry	Enables retry attempts after a failed authentication.
retry count	Number of retry attempts from 0 to 5.
server	Configures the actions for AAA server events.
vlan	Specifies the authentication-fail VLAN.
vlan-id	VLAN ID number from 1 to 4094.
voice	Specifies that if the traffic from the host is tagged with the voice VLAN, the device is placed in the configured voice VLAN on the port.

Defaults

No event responses are configured on the port.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(53)SE2	This command was introduced.
15.0(1)SE	The **voice** keyword was added.

Usage Guidelines

Use this command with the **fail**, **no-response**, or **event** keywords to configure the switch response for a specific action.

For *authentication-fail* events:

- If the supplicant fails authentication, the port is moved to a restricted VLAN, and an EAP success message is sent to the supplicant because it is not notified of the actual authentication failure.
  - If the EAP success message is not sent, the supplicant tries to authenticate every 60 seconds (the default) by sending an EAP-start message.
  - Some hosts (for example, devices running Windows XP) cannot implement DHCP until they receive an EAP success message.

  The restricted VLAN is supported only in single host mode (the default port mode). When a port is placed in a restricted VLAN, the supplicant MAC address is added to the MAC address table. Any other MAC address on the port is treated as a security violation.
- You cannot configure an internal VLAN for Layer 3 ports as a restricted VLAN. You cannot specify the same VLAN as a restricted VLAN and as a voice VLAN.

  Enable re-authentication with restricted VLANs. If re-authentication is disabled, the ports in the restricted VLANs do not receive re-authentication requests.

  To start the re-authentication process, the restricted VLAN must receive a link-down event or an Extensible Authentication Protocol (EAP) logoff event from the port. If a host is connected through a hub:
  - The port might not receive a link-down event when the host is disconnected.
  - The port might not detect new hosts until the next re-authentication attempt occurs.

When you reconfigure a restricted VLAN as a different type of VLAN, ports in the restricted VLAN are also moved and stay in their currently authorized state.

For *no-response* events:

- If you enable a guest VLAN on an IEEE 802.1x port, the switch assigns clients to a guest VLAN when it does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.
- The switch maintains the EAPOL packet history. If another EAPOL packet is detected on the port during the lifetime of the link, the guest VLAN feature is disabled. If the port is already in the guest VLAN state, the port returns to the unauthorized state, and authentication restarts. The EAPOL history is cleared.
- If the switch port is moved to the guest VLAN (multihost mode), multiple non-IEEE 802.1x-capable clients are allowed access. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put in the unauthorized state in the RADIUS-configured or user-configured access VLAN, and authentication restarts.

  You can configure any active VLAN except a Remote Switched Port Analyzer (RSPAN) VLAN, a primary private VLAN, or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is supported only on access ports. It is not supported on internal VLANs (routed ports) or trunk ports.
- When MAC authentication bypass is enabled on an IEEE 802.1x port, the switch can authorize clients based on the client MAC address if IEEE 802.1x authentication times out while waiting for an EAPOL message exchange. After detecting a client on an IEEE 802.1x port, the switch waits for an Ethernet packet from the client. The switch sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address.
  - If authorization succeeds, the switch grants the client access to the network.
  - If authorization fails, the switch assigns the port to the guest VLAN if one is specified.

  For more information, see the "Using IEEE 802.1x Authentication with MAC Authentication Bypass" section in the "Configuring IEEE 802.1x Port-Based Authentication" chapter of the software configuration guide.

For *server-dead* events:

- When the switch moves to the critical-authentication state, new hosts trying to authenticate are moved to the critical-authentication VLAN (or *critical VLAN*). This applies whether the port is in single-host, multiple-host, multi-auth, or MDA mode. Authenticated hosts remain in the authenticated VLAN, and the reauthentication timers are disabled.
- If a client is running Windows XP and the critical port to which the client is connected is in the critical-authentication state, Windows XP might report that the interface is not authenticated.
- If the Windows XP client is configured for DHCP and has an IP address from the DHCP server and a critical port receives an EAP-Success message, the DHCP configuration process might not re-initiate.

You can verify your settings by entering the **show authentication** privileged EXEC command.

Examples

This example shows how to configure the **authentication event fail** command:

```
Switch(config-if)# authentication event fail action authorize vlan 20
```

This example shows how to configure a no-response action:

```
Switch(config-if)# authentication event no-response action authorize vlan 10
```

This example shows how to configure a server-response action:

```
Switch(config-if)# authentication event server alive action reinitialize
```

This example shows how to configure a port to send both new and existing hosts to the critical VLAN when the RADIUS server is unavailable. Use this command for ports in multiple authentication (multi-auth) mode or if the voice domain of the port is in MDA mode:

```
Switch(config-if)# authentication event server dead action authorize vlan 10
```

This example shows how to configure a port to send both new and existing hosts to the critical VLAN when the RADIUS server is unavailable and if the traffic from the host is tagged with the voice VLAN to put the host in the configured voice VLAN on the port. Use this command for ports in multiple-host or multiauth mode:

```
Switch(config-if)# authentication event server dead action reinitialize vlan 10
Switch(config-if)# authentication event server dead action authorize voice
```

Related Commands

Command	Description
authentication control-direction	Configures the port mode as unidirectional or bidirectional.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port.
show authentication	Displays information about authentication manager events on the switch.

dot1x supplicant controlled transient

To control access to an 802.1x supplicant port during authentication, use the **dot1x supplicant controlled transient** command in global configuration mode. To open the supplicant port during authentication, use the **no** form of this command

dot1x supplicant controlled transient

no dot1x supplicant controlled transient

Syntax Description

This command has no arguments or keywords.

Defaults

Access is allowed to 802.1x supplicant ports during authentication.

Command Modes

Global configuration

Command History

Release	Modification
15.0(1)SE	This command was introduced.

Usage Guidelines

In the default state, when you connect a supplicant switch to an authenticator switch that has BPCU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** global configuration command temporarily blocks the supplicant port during authentication to ensure that the authenticator port does not shut down before authentication completes. If authentication fails, the supplicant port opens. Entering the **no dot1x supplicant controlled transient** global configuration command opens the supplicant port during the authentication period. This is the default behavior.

We strongly recommend using the **dot1x supplicant controlled transient** command on a supplicant switch when BPDU guard is enabled on the authenticator switch port with the **spanning-tree bpduguard enable** cinterface onfiguration command.

Note If you globally enable BPDU guard on the authenticator switch by using the **spanning-tree portfast bpduguard default** global configuration command, entering the **dot1x supplicant controlled transient** command does not prevent the BPDU violation.

Examples

This example shows how to control access to 802.1x supplicant ports on a switch during authentication:

```
Switch(config)# dot1x supplicant controlled transient
```

Related Commands

Command	Description
cisp enable	Enables Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
dot1x credentials	Configures the 802.1x supplicant credentials on the port.
dot1x pae supplicant	Configures an interface to act only as a supplicant.

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 for Cisco IOS Release 15.0(1)SE

Platform FRULink 10G Service Module Messages

Error Message `LICENSE,PLATFORM_SM10G-0-LOG_INFO:FRULink 10G Service Module (C3KX-SM-10G) features are not supported with this license level. Module is in pass-thru mode.`

Explanation The services and features of the service module require an IP base or IP services license level. If this license is not installed and activated, the module operates only in pass-through mode.

Recommended Action Install or activate an IP base or IP services license.

Error Message `HARDWARE,PLATFORM_SM10G-0-LOG_ERR: FRULink 10G Service Module (C3KX-SM-10G) features are not supported on this revision of switch hardware. Please upgrade the switch hardware to use the module's features.`

Explanation The module requires an internal switch hardware version newer than the current version. The switch hardware must be upgraded to support the service module features.

Recommended Action Contact Cisco and upgrade the switch hardware.

Error Message `NO_RESPONSE,PLATFORM_SM10G-0-LOG_ERR: The FRULink 10G Service Module (C3KX-SM-10G) is not responding.`

Explanation The service module is not responding. This could be due to hardware or software failure or a module reload.

Recommended Action Reboot or replace the service module.

Error Message `AUTHENTICATION,PLATFORM_SM10G-0-LOG_ERR: The FRULink 10G Service Module (C3KX-SM-10G) may not have been entirely manufactured by Cisco. Module is in pass-through mode.`

Explanation A portion of the service module hardware could not be verified as Cisco hardware. Extended services and features are disabled, and the module can operate only in pass- through mode.

Recommended Action Contact Cisco and replace the service module.

Error Message `SW_VERSION_MISMATCH,PLATFORM_SM10G-0-LOG_ERR: The FRULink 10G Service Module (C3KX-SM-10G) software version is incompatible with the IOS software version. Please update the software. Module is in pass-thru mode.`

Explanation The Cisco IOS software and the FRULink 10G service module software are incompatible.

Recommended Action Upgrade the switch or service module software so that the versions are compatible.

Error Message `FPGA_UPDATE_INITIATED,PLATFORM_SM10G-0LOG_ERR: The FRULink 10G Service Module (C3KX-SM-10G) firmware is being updated due to a version mismatch. Please wait a few minutes for the update to complete.`

Explanation The firmware was corrupted and is being restored.

Recommended Action Wait for the firmware upgrade to complete.

Error Message `FPGA_RELOADED,PLATFORM_SM10G-0-LOG_ERR: The FRULink 10G Service Module (C3KX-SM-10G) firmware has been updated and the module will be reloaded.`

Explanation The firmware was corrupted and has been restored.

Recommended Action No action is required.

Error Message `FPGA_RELOAD_FAILED,PLATFORM_SM10G-0-LOG_ERR: The FRULink 10G Service Module (C3KX-SM-10G) firmware could not be updated.`

Explanation The firmware image has been corrupted and could not be restored.

Recommended Action Contact Cisco and replace the service module.

Error Message `CORRUPT_SW_IMAGE,PLATFORM_SM10G-0-LOG_ERR: The FRULink 10G Service Module (C3KX-SM-10G) software version is corrupted. Please update the software. Module is in pass-thru mode.`

Explanation The FRULink 10G service module software is invalid.

Recommended Action Update the service module software.

Error Message `LINK_UP,PLATFORM_SM10G-0-LOG_INFO: The FRULink 10G Service Module (C3KX-SM-10G) communication has been established`

Explanation The service module has established communication with the switch.

Recommended Action No action is required. Information only message.

New System Messages for Cisco IOS Release 12.2(58)SE

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 occured 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]s 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.