Release Notes for the Catalyst 3750-X and 3560-X Switches, Cisco IOS Release 15.2(3)E and Later

First Published: December 10, 2014

Last Updated: January 15, 2016

Cisco IOS Release 15.2(3)E and later runs on Catalyst 3750-X and Catalyst 3650-X switches and on Cisco enhanced EtherSwitch service modules.

The Catalyst 3750-X switch supports stacking through Cisco StackWise Plus technology and also supports StackPower. The Catalyst 3560-X 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.

For more information, see the Deciding Which Files to Use, page 8 and the "Caveats" section on page 27.

These release notes include important information about Cisco IOS release 15.2(3)E 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 7.
- 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 8.

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

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
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

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

Switch Model	Description	Supported by Minimum Cisco IOS Release
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(55)SE5
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(55)SE5
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(55)SE5
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(55)SE5
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
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

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

Switch Model	Description	Supported by Minimum Cisco IOS Release
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
Catalyst 3750-X-24-U-L	24 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; LAN Base feature set	15.0(2)SE
Catalyst 3750-X-48-U-L	48 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; LAN Base feature set	15.0(2)SE
Catalyst 3750-X-24-U-S	24 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; IP Base feature set	15.0(2)SE
Catalyst 3750-X-48-U-S	48 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; IP Base feature set	15.0(2)SE
Catalyst 3750-X-24-U-E	24 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; IP Services feature set	15.0(2)SE
Catalyst 3750-X-48-U-E	48 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; IP Services feature set	15.0(2)SE
Catalyst 3560-X-24-U-L	24 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; LAN Base feature set	15.0(2)SE
Catalyst 3560-X-48-U-L	48 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; LAN Base feature set	15.0(2)SE
Catalyst 3560-X-24-U-S	24 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; IP Base feature set	15.0(2)SE
Catalyst 3560-X-48-U-S	48 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; IP Base feature set	15.0(2)SE
Catalyst 3560-X-24-U-E	24 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; IP Services feature set	15.0(2)SE

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

Switch Model	Description	Supported by Minimum Cisco IOS Release
Catalyst 3560-X-48-U-E	48 10/100/1000 Universal PoE ports, EEE support, 1 network module slot, 1100 W power supply; IP Services feature set	15.0(2)SE
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 DWDM	12.2(53)SE2
SFP+ Modules	SFP-10G-ER[4]	15.0(2)SE
Support for these SFP+ modules	Only version 02 (or later) of the CX1[5] cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	12.2(53)SE2
SFP module patch cable[6]	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

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

Switch Model	Description	Supported by Minimum Cisco IOS Release
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	2X1G/2X10G Fibre uplink service module	15.0(1)SE
eXpandable power system (XPS)	Cisco XPS 2200	12.2(55)SE1
SM-X-ES3-24-P-T	EtherSwitch SM L3 + PoEPlus + MACSec + 24 10/100/1000 (Temperature hardended)	15.2(2)E1
SFP+ module	SFP-10G-ZR	15.2(3)E

1. PoE+ = Power over Ethernet, up to 30 W per port
2. CWDM = coarse wavelength-division multiplexer
3. DWDM = dense wavelength-division multiplexer
4. Only for Catalyst 3560-X and 3750-X switches
5. The CX1 cables are used with the OneX converters.
6. Only Catalyst 3560-X switches. The SFP module patch cable is a 0.5-meter, copper, passive cable with SFP module connectors at each end. The patch cable can be used in 1 Gigabit Ethernet SFP ports to connect two Catalyst 3560-X switches in a cascaded configuration. You can use the patch cable with the 10 G network module only on SFP ports 1 and 3 (not on SFP+ ports 2 and 4).

Device Manager System Requirements

Hardware

Table 2 Minimum Hardware Requirements

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

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

Software

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 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 15.2(2)E will be supported in a future release of the Cisco Network Assistant. Cisco IOS 12.2(35)SE2 and later is compatible only 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.

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.

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 3 Software Images

Image	Filename	Description
Catalyst 3750-X and Catalyst 3560-X switches		
Universal without payload encryption	c3560e-universalk9npe-mz.152-3.E1.bin c3560e-universalk9npe-tar.152-3.E1.tar c3750e-universalk9npe-mz.152-3.E1.bin c3750e-universalk9npe-tar.152-3.E1.tar	All the supported universal image features, Kerberos, SSH, SSL, and SNMPv3 LAN base, IP base, and IP services software licenses

Table 3 Software Images (continued)

Image	Filename	Description
Universal with payload encryption	c3560e-universalk9-mz.152-3.E1.bin c3560e-universalk9-tar.152-3.E1.tar c3750e-universalk9-mz.152-3.E1.bin c3750e-universalk9-tar.152-3.E1.tar	All the supported universal image features, Kerberos, SSH, SSL, SNMPv3, and MACsec LAN base, IP base, and IP services software licenses
	c3kx-sm10g-tar.152-3.E1.tar c3kx-sm10g-tar.152-3.E1.tar	

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 3 on page 8 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.

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

Features Introduced in Cisco IOS Release 15.2(3)E3

What's new	Description
Enhancement to Web-auth configuration	(IP Base) Commands under global parameter-map to enable non SVI and VRF aware Web-auth configuration.
Rapid PVST+	(All licenses) Rapid PVST+ is now the default spanning-tree mode used on all Ethernet port-based VLANs
Enhancement to Smart Install	(All licenses) PnP discovery process via various discovery mechanisms and security methods is supported
Named VLAN	(All licenses) Option to specify a VLAN name for access and voice VLAN.

Features Introduced in Cisco IOS Release 15.2(3)E2

There are no new features to mention here.

Features Introduced in Cisco IOS Release 15.2(3)E1

What's New	Description
Enhancement to port security configuration	Specify a MAC address that is forbidden by port security on all interfaces.

Features Introduced in Cisco IOS Release 15.2(3)E

What's New	Description
IPv6 First Hop Security support on Etherchannels	The IPv6 FHS policies can be attached to EtherChannel interfaces (Port Channels).
Auto-QoS Compact	This feature hides the auto-QoS-generated commands from the running configuration.
VLAN name extension	Maximum characters allowed for a VLAN name has been increased from 32 to 128.
mDNS Service Discovery Gateway Phase 3	The Service Discovery Gateway feature enables multicast Domain Name System (mDNS) to operate across Layer 3 (L3) boundaries. In this phase, features such as de-congestion of incoming mDNS traffic, redistribution of service withdrawal messages, a filter criterion for learning services available on a specific interface, and the periodic browsing of services on specific interfaces are introduced.
LDAP source interface and VRF support	Allows you to configure a dedicated LDAP source interface IP address and virtual routing and forwarding (VRF).
AN Infra	Autonomic networking makes network devices intelligent by introducing self-management concepts that simplify network management for the network operator.
VRF aware DHCPv6 Server/Relay for Prefix Delegation	Ensures that the DHCPv6 server and relay involved in delegating prefixes are VRF aware.
VRF aware DHCPv6 server/Relay for IANA	Ensures that the DHCPv6 server and relay used for IP address provision are VRF aware.
BFD support for ISIS IPv4 and IPv6	Enables Intermediate System-to-Intermediate System (IS-IS) to use Bidirectional Forwarding Detection (BFD) support, which improves IS-IS convergence as BFD detection and failure times are faster than IS-IS convergence times in most network topologies. This feature also enables the network to identify whether a BFD session failure is genuine or is the result of a control plane failure due to a router restart.
VLAN RADIUS Attributes in Access Requests	Enhances the security for access switches with the use of VLAN RADIUS attributes (VLAN name and ID) in the access requests and with an extended VLAN name length of 128 characters.
Copy Aware VRF	Enables copying of files to and from a VRF via the **copy** command.

Minimum Cisco IOS Release for Major Features

Table 4 lists the minimum software release after the first release of required to support the major features on the switches. The first release of the Catalyst 3750-X and 3560-X switches was Cisco IOS Release 12.2(53)SE2).

Table 4 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-X, 3560-X
NEAT enhancement to control access to the supplicant port	15.0(1)SE	3750-X, 3560-X
Cisco TrustSec SXP version 2, syslog messages, and SNMP support	15.0(1)SE	3750-X, 3560-X
Auto Smartports improved device classification	15.0(1)SE	3750-X, 3560-X
Device Sensor	15.0(1)SE	3750-X, 3560-X
Built-in Traffic Simulator using Cisco IOS IP SLAs video operations	12.2(58)SE1	3750-X, 3560-X
Cisco Mediatrace support	12.2(58)SE1	3750-X, 3560-X
Cisco performance monitor	12.2(58)SE1	3750-X, 3560-X
EnergyWise Phase 2.5	12.2(58)SE1	3750-X, 3560-X
Smart logging	12.2(58)SE1	3750-X, 3560-X
Protocol storm protection	12.2(58)SE1	3750-X, 3560-X
VACL Logging	12.2(58)SE1	3750-X, 3560-X
Smart Install 3.0	12.2(58)SE1	3750-X, 3560-X
Auto Smartports enhancements to enable auto-QoS on a digital media player.	12.2(58)SE1	3750-X, 3560-X
Memory consistency check routines	12.2(58)SE1	3750-X, 3560-X
Call Home support	12.2(58)SE1	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-X, 3560-X
NTP version 4	12.2(58)SE1	3750-X, 3560-X
DHCPv6 bulk-lease query and DHCPv6 relay source configuration	12.2(58)SE1	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-X, 3560-X
RADIUS, TACACS+, and SSH/SCP over IPv6	12.2(58)SE1	3750-X, 3560-X
VRRP for IPv4	12.2(58)SE1	3750-X, 3560-X
IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates	12.2(58)SE1	3750-X, 3560-X
Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices.	12.2(55)SE	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-X, 3560-X
CDP and LLDP enhancements for exchanging location information with video end points.s.	12.2(55)SE	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-X, 3560-X

Table 4 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Dynamic creation or attachment of an auth-default ACL on a port with no configured static ACLs.	12.2(55)SE	3750-X, 3560-X
VLAN assignment on a port configured for multi-auth mode.	12.2(55)SE	3750-X, 3560-X
EEM in IP base image.	12.2(55)SE	3750-X, 3560-X
IP base support for OSPF routed access.	12.2(55)SE	3750-X, 3560-X
Cisco TrustSec SXP.	12.2(55)SE 12.2(53)SE2	3750-X, 3560-X

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

- 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)

- Standalone web-based authentication fails if the switch port is configured without any port ACL. (CSCuu91975)

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 Transceiver Modules and SFP Modules

- 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)

- 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

- 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 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)

- When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may crash. As a workaround, disable the logging discriminator on the device (CSCur45606, CSCur28336).

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)

- When configuring queuing policy, the sum of the queuing buffer should not exceed 100%.

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)

- 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 the RSPAN feature is configured on a switch, CDP packets received from the RSPAN source ports are tagged with the RSPAN VLAN ID and forwarded to trunk ports carrying the RSPAN VLAN. When this happens, a switch that is more than one hop away incorrectly lists the switch that is connected to the RSPAN source port as a CDP neighbor.

  This is a hardware limitation. The workaround is to disable CDP on all interfaces carrying the RSPAN VLAN on the device connected to the switch. (CSCeb32326)

- 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 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 only if the monitor source port(s) is a pluggable Gigabit module and you set any source port combination, except when just using a single Gigabit port on the pluggable module as the source port.

  This is a cosmetic issue and 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 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)

- 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)

- 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)

- 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)

TrustSec

The following guidelines and limitations apply to configuring Cisco TrustSec SGT and SGACL on the Catalyst 3750-X switch:

- You cannot statically map an IP-subnet to an SGT. You can only map IP addresses to an SGT. When you configure IP address-to-SGT mappings, the IP address prefix must be 32.
- If a port is configured in Multi-Auth mode, all hosts connecting on that port must be assigned the same SGT. When a host tries to authenticate, its assigned SGT must be the same as the SGT assigned to a previously authernticated host. If a host tries to authenticate and its SGT is different from the SGT of a previously authenticated host, the VLAN port (VP) to which these hosts belong is error-disabled.
- Cisco TrustSec enforcement is supported only on up to eight VLANs on a VLAN-trunk link. If there are more than eight VLANs configured on a VLAN-trunk link and Cisco TrustSec enforcement is enabled on those VLANs, the switch ports on those VLAN-trunk links will be error-disabled.
- The switch cannot assign an SGT based on SXP listening; it can only forward the SXP bindings through the SXP protocol.
- Port-to-SGT mapping should be configured only on Cisco TrustSec links (that is, switch-to-switch links).

  When port-to-SGT mapping is configured on a port, an SGT is assigned to all ingress traffic on that port. There is no SGACL enforcement for egress traffic on the port.
- SGT/SGACL is supported on Cisco Catalyst 3750-X and 3650-X series switches with all network uplink modules: C3KX-NM-1G, C3KX-NM-10G, C3KX-NM-10GT and C3KX-SM-10G. The C3KX-SM-10G is only required for MACsec on the uplinks.
- TrustSec Layer-3 Identity Port Mapping (L3IPM) is not supported on Catalyst 3750-X and 3650-X series switches.

IP SLA Video Operation

- After removing an IP SLA Video Operation VRF configuration, the VRF configuration still shows up in **show running-config** and **show ip sla configuration**. The VRF configuration is removed, but the CLI is not updated.

  The workaround is to completely remove the IP SLA Video Operation and configure again without VRF. (CSCuf39077)

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

- 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)

- Cisco Trust Security (CTS) MACsec cannot be configured on the C3KX-SM-10G service module until the POST test has been completed. Wait approximately 45 seconds after the module is inserted before you configure CTS MACsec on the port. (CSCuc20819)

Important Notes

Switch Stack Notes

- Always power off a switch before adding or removing it from a switch stack.

Control Plane Protection

Catalyst 3750-X and 3560-X 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.

Caveats

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats

Bug ID	Headline
CSCum91247	ARP Cache storm locks up switch - power cycle required to recover

Caveats Resolved in Cisco IOS Release 15.2(3)E3

Bug ID	Headline
CSCur23262	On removing 8 queue with AQC enabled, will remove the auto qos
CSCus32213	CTS Manual is not working with legacy 3750x Vs 3560x with 15.2(3)E
CSCuu16044	3750 - Not Processing LACP PDUs if Native VLAN is not created
CSCuu92224	2960X - EPM vlan plugin crash
CSCuu97550	4500X - SNMP dot1dTpFdbPort retuning incorrect value
CSCuv05123	c3560e/v151_sy_throttle platform doesn't store NTP drift values properly
CSCuv32909	3560X crash occurred with %BIT-4-OUTOFRANGE message after doing show run
CSCuv50743	MAC stuck on 'PRE Event Handling' - needs reload for recover
CSCuw17699	Switch crashes with Data TLB Miss Exception
CSCuw39020	access-session vlan-assignment ignore-errors breaks dynamic vlan assign
CSCuw44957	Cat3560X:some fragmented packets drop
CSCuw71607	Switch crashed at HLFM aging process
CSCuw71809	There is no warning message when the C3K configures "ip tcp adjust-mss"

Caveats Resolved in Cisco IOS Release 15.2(3)E2

Bug ID	Headline
CSCun85734	SNMP:ctspAuthorizationSgaclFailNotif notification is disabled.

Caveats Resolved in Cisco IOS Release 15.2(3)E1

Bug ID	Headline
CSCtg15739	Failed sessions are not removed in multi-auth mode
CSCup68355	Stack members fail on Etherchannel ports in C3KX-SM-10G or downlinks.
CSCur17365	15.2(2)E: CSCup68355 verification errdisabled pagp-flap between 3750x and 2960s
CSCur64486	Switch is unable to send packets with payload larger than 1496 bytes.

Caveats Resolved in Cisco IOS Release 15.2(3)E

Bug ID	Headline
CSCto97888	GLC-BX-D/U, CWDM, DWDM SFP in ports 2 and 4 of C3KX-NM-10G don't linkup
CSCuh17594	UDP Jitter probes may return erroneously low or high RTT values
CSCuh65490	Memory leak - qos_set_if_t,qos set codepoint on 2K/3K stack
CSCui16394	WS-C3750X-12S does not forward packets(over 1300 bytes) through 10M port
CSCui21029	3750X Stack no standalone stays in running configureation as standalone
CSCuj74358	CLI to enable flooding of multicast on portfast ports
CSCum27170	Cannot poll VRF routes using ipCidrRouteTable
CSCum72168	High CPU caused due to snmpwalk on cbQosPoliceActionCfgEntry
CSCum89956	Stack ping failed on int has static mac bounded after removed cable
CSCun01172	kSlow CLI response when configuring 3750X stacked switches
CSCun25154	DHCP client behaviour change between 15.0(2)SE2 and 15.0(2)SE4
CSCun26893	High CPU due to ASP Process Crea, crash on disabling macros
CSCun34745	"ip ssh source-interface" configuration missing after reload
CSCuo03803	SSTE: Amur: ENTROPY-0-ENTROPY_ERROR: Unable to collect sufficient
CSCuo13242	Re-authentication fails after clear authentication sessions command
CSCuo17293	MAC sync issue on 3750 stack running SE5
CSCuo31164	match prefix is removed from SNMP V3 configuration after host command
CSCuo48542	Need to make test macsec CLI Syndrome aware
CSCuo50456	WS-C3560X high CPU with REP LSL Hello PP Process during failover
CSCuo58284	UDP fragment drop with "Unknown IPC message type" after switchover
CSCuo62332	CISCO-BGP-MIBv8.1 - Add support for cbgpPeer2Type in BGP traps/notif
CSCuo66933	Switch sent Failure packet after reboot and caused PC to fail authen
CSCuo73442	Switch crash after 'no ip dhcp pool' command
CSCuo95181	Group specific Query with Router alert option dropped.
CSCuo97298	PS-FAN falls to FAUTY status after upgrading IOS.
CSCup49030	EX90/60 can't get ip via DHCP in data vlan
CSCup52101	EnergyWise Denial of Service vulnerabilty

Bug ID	Headline
CSCup55822	Delays in Convergence time during link-flap between VSS and 3750
CSCup58066	"show LLDP neighbors" truncates Device ID if the hostname contains "."
CSCup68355	Amur:3750X/2960s crash w/. creating EC part of walle module or downlinks
CSCup79358	C3KX-SM-10G doesn't pass through any packets after reloading switch
CSCup86619	Port err-disable after link-flap with "speed nonegotiate" option.
CSCup86666	Configuration "no logging event link-status" can't be deleted.
CSCup96299	IPv6 Multicast RIB entry refer to wrong distance
CSCuq03344	Multicast traffic drops although multicast entry exists on the table.
CSCuq06262	VTP status not sync between the stack master and slave
CSCuq10827	C3560X cHsrpGrpStandbyState is incorrect
CSCuq11337	Fail to bundle l2protocol ports into channel
CSCuq12940	description under "no switchport" interface lost in show run
CSCuq23741	3750 - not processing VLAN 1 BPDU if Native VLAN is not created
CSCuq27324	Crash after mls qos dscp-mutation
CSCuq49531	10G link convergence is better than 1G convergence when is link pulled
CSCuq58584	UDP(1975) causes Error msg %IPC-2-INVALIDZONE: Invalid IPC Zone on 3750X
CSCuq67809	3750x stack crashes with to big buffer allocated
CSCur43620	%PLATFORM_IPC-3-COMMON: Unknown IPC message type 65535 size 91

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.

These documents that provide 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

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*
- *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.
