Release Notes for Catalyst 3750-E and 3560-E Switches, Cisco IOS Release 12.2(52)SE, and for Cisco Enhanced EtherSwitch Service Modules, Cisco IOS Release 12.2(52)EX and Later

Revised May 24, 2010

Cisco IOS Release 12.2(52)SE and later runs on Catalyst 3750-E and Catalyst 3560-E switches. Cisco IOS Release 12.2(52)EX and later runs on Cisco enhanced EtherSwitch service modules.

The Catalyst 3750-E switches support stacking through Cisco StackWise Plus technology. The Catalyst 3560-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.

For more information, see the Deciding Which Files to Use, page 7 and the "Documentation Updates" section on page 33.

These release notes include important information about Cisco IOS Release 12.2(52)SE and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 6.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 7.

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

http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches

This software release is part of a special release of Cisco IOS software that is not released on the same maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

For the complete list of Catalyst 3750-E and Catalyst 3560-E switch documentation and of Cisco enhanced EtherSwitch service module documentation, see the "Related Documentation" section on page 42.

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

Contents

This information is in the release notes:

System Requirements

The system requirements are described in these sections:

Hardware Supported

Table 1 lists the hardware supported on this release.

Table 1 Catalyst 3750-E and 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

Table 1 Catalyst 3750-E and 3560-E Switches and Cisco Enhanced EtherSwitch Service Module Supported Hardware (continued)

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
Cisco 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	Cisco IOS Release 12.2(35)SE2
	X2-10GB-LRM	Cisco IOS Release 12.2(40)SE
	10 Gigabit Ethernet X2 ZR optical modules	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 1 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 CWDM[3] For a complete list of supported SFPs and part numbers, see the data sheet at: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps7077/product_data_sheet0900aecd805bbe67.html	Cisco IOS Release 12.2(35)SE2
DOM[4] support for these SFP modules	X2-10GB-ER, X2-10GB-SR, X2-10GB-LR, X2-10GB-LRM, 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
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[6]	48 10/100 ports, 2 SFP module slots	12.2(52)EX
SM-D-ES3-48-P[6]	48 10/100 ports with PoE, 2 SFP module slots	12.2(52)EX
SM-D-ES3G-48-P[6]	48 10/100/1000 with PoE, 2 SFP module slots	12.2(52)EX
SM-ES2-16-P[6]	15 10/100 ports with PoE, 1 10/100/1000 port with PoE	12.2(52)EX
SM-ES2-24[6]	23 10/100 ports, 1 10/100/1000 port	12.2(52)EX

Table 1 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-P[6]	Layer 2-capable, 23 10/100 ports with PoE, 1 10/100/1000 port with PoE	12.2(52)EX
SM-ES3-16-P[6]	15 10/100 ports with PoE, 1 10/100/1000 port with PoE	12.2(52)EX
SM-ES3-24-P[6]	23 10/100 ports with PoE, 1 10/100/100 port with PoE	12.2(52)EX
SM-ES3G-16-P[6]	16 10/100/1000 ports with PoE	12.2(52)EX
SM-ES3G-24-P[6]	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. Cisco enhanced EtherSwitch service module

Device Manager System Requirements

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

- "Hardware Requirements" section on page 5
- "Software Requirements" section on page 5

Hardware Requirements

Table 2 lists the minimum hardware requirements for running the device manager.

Table 2 Minimum Hardware Requirements

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

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

Software Requirements

These are the supported operating systems and browsers for the device manager:

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

The device manager verifies the browser version when starting a session, and it 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-E switch, all standby command switches must be Catalyst 3750-E switches.

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

CNA Compatibility

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

http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

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

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- "Finding the Software Version and Feature Set" section on page 6
- "Deciding Which Files to Use" section on page 7
- "Upgrading a Switch by Using the Device Manager or Network Assistant" section on page 8
- "Upgrading a Switch by Using the CLI" section on page 9
- "Recovering from a Software Failure" section on page 10

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

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 3 Cisco IOS Software Image Files

Filename	Description
c3750e-ipbase-tar.122-52.SE.tar	Catalyst 3750-E IP base image and device manager files. This image has Layer 2+ and basic Layer 3 routing features.
c3750e-universal-tar.122-52.SE.tar	Catalyst 3750-E universal image and device manager files. This image has all the supported features that are enabled by the installed software license.
c3750e-ipbasek9-tar.122-52.SE.tar	Catalyst 3750-E IP base cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, Layer 2+, and basic Layer 3 routing features.
c3750e-universalk9-tar.122-52.SE.tar	Catalyst 3750-E universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, SNMPv3, and supported universal image features.
c3560e-ipbase-tar.122-52.SE.tar	Catalyst 3560-E IP base image and device manager files. This image has Layer 2+ and basic Layer 3 routing features.
c3560e-universal-tar.122-52.SE.tar	Catalyst 3560-E universal image and device manager files. This image has all the supported features that are enabled by the installed software license. This image also runs on these Cisco enhanced EtherSwitch 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.
c3560e-ipbasek9-tar.122-52.SE.tar	Catalyst 3560-E IP base cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, Layer 2+, and basic Layer 3 routing features.
c3560e-universalk9-tar.122-52.SE.tar	Catalyst 3560-E universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, and SNMPv3, and supported universal image features. This image also runs on these Cisco enhanced EtherSwitch 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.

Table 3 Cisco IOS Software Image Files (continued)

Filename	Description
c2960sm-lanbase-tar.122-52.EX1.tar	Image file and device manager files for these Cisco enhanced EtherSwitch service modules: SM-D-ES2-48, SM-ES2-16-P, SM-ES2-24, and SM-ES2-24-P6. This image has Layer 2+ features.
c2960sm-lanbasek9-tar.122-52.EX1.tar	Cryptographic image file and device manager files for these Cisco enhanced EtherSwitch service modules: SM-D-ES2-48, SM-ES2-16-P, SM-ES2-24, and SM-ES2-24-P6. This image has the Kerberos and SSH features.

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

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

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release from which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time-consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2,* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800811e0.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. For detailed instructions, click **Help**.

Note When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

Step 1 Use Table 3 on page 7 to identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

To download the universal software image files for a Catalyst 3750-E switch, click **Catalyst 3750-E software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3750-E 3DES Cryptographic Software**.

To download the universal software image files for a Catalyst 3560-E switch, click **Catalyst 3560-E software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3560-E 3DES Cryptographic Software**.

To download the universal software image files for a SM-D-ES2-48, SM-ES2-16-P, SM-ES2-24, or SM-ES2-24-P6 module, click **Catalyst 2960SM software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2960SM 3DES Cryptographic Software**.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, see Appendix B in the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For **//***location*, specify the IP address of the TFTP server.

For */directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/c3750e-universal-tar.122-50.SE.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

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

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Features

These sections describe the new supported hardware and the new and updated software features provided in this release:

- "New Hardware Features" section on page 10
- "New Software Features" section on page 10

New Hardware Features

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

New Software Features

- Full QoS support for IPv6 traffic.
- The command 'ip tcp adjust-mss' is not supported on the 3750x/3560x/3750g/3560g/3750e/3560e platforms.
- Smart Install to allow a single point of management (director) in a network. You can use Smart Install to provide zero touch image and configuration upgrade of newly deployed switches and image and configuration downloads for any client switches

- Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications. One of the services of Medianet is auto provisioning for Cisco Digital Media Players and Cisco IP Video Surveillance cameras through Auto Smartports.
- AutoSmartPort enhancements, which adds support for macro persistency, LLDP-based triggers, MAC address and OUI-based triggers, remote macros as well as for automatic configuration based on these two new device types: Cisco Digital Media Player (Cisco DMP) and Cisco IP Video Surveillance Camera (Cisco IPVSC).
- Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.
- Support for IP source guard on static hosts.
- RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Secure ACS to reinitialize authentication, and apply to the new policies.
- IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.
- Customizable web authentication enhancement to allow the creation of user-defined *login*, *success*, *failure* and *expire* web pages for local web authentication.
- Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.
- VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.
- MAC move to allow hosts (including the hosts connected behind the phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.
- Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.
- DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.
- Increased support for LLPD-MED by allowing the switch to grant power to the power device (PD), based on the power policy TLV request.
- Support for VTP version 3 that includes support for configuring extended range VLANs (VLANs 1006 to 4094) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port.
- Support for QoS marking of CPU-generated traffic and queue CPU-generated traffic on the egress network ports.

- Shorter Resilient Ethernet Protocol (REP) hello: Changes the range of the REP link status layer (LSL) age timer from 3000 to 10000 ms in 500-ms intervals to 120 to 10000 ms in 40-ms intervals.
- Cisco EnergyWise to manage the power usage of EnergyWise entities, such as power over Ethernet (PoE) devices.
- Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.
- Support for up to 32 10 Gigabit Ethernet DWDM X2 optical modules.
- Support for eight additional DWDM SFP optical modules. For a complete list of supported SFPs and part numbers, see the data sheet at:

  http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps7077/product_data_sheet0900aecd805bbe67.html

Minimum Cisco IOS Release for Major Features

Table 4 lists the minimum software release (after the first release) required to support the major features of the Catalyst 3750-E and Catalyst 3560-E switches. Features not listed are supported in all releases.

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

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
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. You can use Smart Install to provide zero touch image and configuration upgrade of newly deployed switches and image and configuration downloads for any client switches.	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. One of the services of Medianet is auto provisioning for Cisco Digital Media Players and Cisco IP Video Surveillance cameras through Auto Smartports.	12.2(50)SE	3750-E, 3560-E
AutoSmartPort enhancements, which adds support for macro persistency, LLDP-based triggers, MAC address and OUI-based triggers, remote macros as well as for automatic configuration based on these two new device types: Cisco Digital Media Player (Cisco DMP) and Cisco IP Video Surveillance Camera (Cisco IPVSC).	12.2(52)SE	3750-E, 3560-E
Support for EEM 3.2, which introduces event detectors for 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) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Secure ACS to reinitialize authentication, and apply to the new policies.	12.2(52)SE	3750-E, 3560-E
IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.	12.2(52)SE	3750-E, 3560-E

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
Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.	12.2(52)SE	3750-E, 3560-E
Customizable web authentication enhancement to allow the creation of user-defined *login*, *success*, *failure* and *expire* web pages for local web authentication.	12.2(52)SE	3750-E, 3560-E
Support for 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 to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.	12.2(52)SE	3750-E, 3560-E
MAC move to allow hosts (including the hosts connected behind the phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.	12.2(52)SE	3750-E, 3560-E
Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.	12.2(52)SE	3750-E, 3560-E
Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.	12.2(52)SE	3750-E, 3560-E
DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE	3750-E, 3560-E
Increased support for LLPD-MED by allowing 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
Support for VTP version 3 that includes support for configuring extended range VLANs (VLANs 1006 to 4094) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port.	12.2(52)SE	3750-E, 3560-E
Support for QoS marking of CPU-generated traffic and queue CPU-generated traffic on the egress network ports.	12.2(52)SE	3750-E, 3560-E
Cisco EnergyWise to manage the power usage of EnergyWise entities, such as power over Ethernet (PoE) devices.	12.2(52)SE	3750-E, 3560-E
Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch	12.2(52)SE	3750-E, 3560-E

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
IEEE 802.1x with open access to allow a host to access the network before being authenticated	12.2(52)SE	3750-E, 3560-E
IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch	12.2(52)SE	3750-E, 3560-E
Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host	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
Cisco EnergyWise manages the energy usage of power over Ethernet (PoE) entities	12.2(52)SE	3750-E, 3560-E
Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.	12.2(52)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 sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE)	12.2(50)SE	3750-E, 3560-E
Intermediate System-to-Intermediate System (IS-IS) routing supports dynamic routing protocols 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 referred to as the Cisco IOS CNS agent	12.2(50)SE	3750-E, 3560-E
Support for Embedded Event Manager Version 2.4	12.2(50)SE	3750-E, 3560-E
LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode	12.2(50)SE	3750-E, 3560-E
RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group	12.2(50)SE	3750-E, 3560-E
Auto Smartports Cisco-default and user-defined macros for dynamic port configuration based on the device type detected on the port	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
These IPv6 features are now 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 IEEE 802.1x and mac authentication bypass (MAB) security violation	12.2(46)SE	3750-E, 3560-E
Local web authentication banner	12.2(46)SE	3750-E, 3560-E

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
Support for the CISCO-NAC-NAD and CISCO-PAE MIBs	12.2(46)SE	3750-E, 3560-E
Digital Optical Monitoring (DOM) of connected SFP modules	12.2(46)SE	3750-E, 3560-E
The ability to exclude a port in a VLAN from the SVI line-state up or down calculation	12.2(46)SE	3750-E, 3560-E
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE	3750-E, 3560-E
HSRP for IPv6 (requires the IP services image)	12.2(46)SE	3750-E, 3560-E
Disabling MAC address learning on a VLAN	12.2(46)SE	3750-E, 3560-E
PAgP Interaction with Virtual Switches and Dual-Active Detection	12.2(46)SE	3750-E, 3560-E
Support for rehosting a software license and for using an embedded evaluation software license	12.2(46)SE	3750-E, 3560-E
EOT and IP SLAs EOT static route support	12.2(46)SE	3750-E, 3560-E
DHCP server port-based address allocation	12.2(46)SE	3750-E, 3560-E
DHCP for IPv6 relay, client, server address assignment and prefix delegation (requires the 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
Simple Network and Management Protocol (SNMP) configuration over IPv6 transport	12.2(44)SE	3750-E, 3560-E
IPv6 support for stateless autoconfiguration	12.2(44)SE	3750-E, 3560-E
Flex Link Multicast Fast Convergence	12.2(44)SE	3750-E, 3560-E
IEEE 802.1x readiness check	12.2(44)SE	3750-E, 3560-E
/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

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
SSM PIM protocol	12.2(40)SE	3750-E, 3560-E
Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6	12.2(40)SE	3750-E, 3560-E
Support for VRF-aware services	12.2(40)SE	3750-E, 3560-E
Support for the Link Layer Discovery Protocol Media Extensions (LLDP-MED) location TLV	12.2(40)SE	3750-E, 3560-E
Support for the CISCO-MAC-NOTIFICATION-MIB	12.2(40)SE	3750-E, 3560-E
Support for the CISCO-POWER-ETHERNET-EXT-MIB	12.2(40)SE	3750-E, 3560-E
DHCP Snooping Statistics **show** and **clear** commands	12.2(37)SE	3750-E, 3560-E
IP phone detection enhancement	12.2(37)SE	3750-E, 3560-E
IP unicast reverse path forwarding (unicast RPF)	12.2(37)SE	3750-E, 3560-E
Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)	12.2(37)SE	3750-E, 3560-E
PIM stub routing in the IP base image	12.2(37)SE	3750-E, 3560-E
Port security on a PVLAN host	12.2(37)SE	3750-E, 3560-E
VLAN aware port security option	12.2(37)SE	3750-E, 3560-E
Support for auto-rendezvous point (auto-RP) for IP multicast	12.2(37)SE	3750-E, 3560-E
VLAN Flex Link Load Balancing	12.2(37)SE	3750-E, 3560-E
Web Cache Communication Protocol (WCCP)	12.2(37)SE	3750-E, 3560-E
SNMP support for the Port Error Disable MIB	12.2(37)SE	3750-E, 3560-E
Support for the Time Domain Reflectometry MIB	12.2(37)SE	3750-E, 3560-E

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

This section contains these limitations:

- "Cisco IOS Limitations" section on page 16
- "Device Manager Limitations" section on page 25

Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 3750-E and 3560-E switches and to the Cisco enhanced EtherSwitch service modules:

- "Access Control List" section on page 17
- "Address Resolution Protocol" section on page 17
- "Cisco Redundant Power System 2300" section on page 17

Access Control List

These are the access control list (ACL) limitations:

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

  There is no workaround. (CSCse33114)

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

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

Address Resolution Protocol

This is an Address Resolution Protocol limitation:

- The switch might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.

  The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem.(CSCse06827))

Cisco Redundant Power System 2300

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

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

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

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

Cisco X2 Transceiver Modules and SFP Modules

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

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

Configuration

These are the configuration limitations:

- 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-E 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)

- 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-E switches)

EtherChannel

These are the EtherChannel limitations:

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

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

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

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

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

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

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

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

  There is no workaround. (CSCsh12472)

IEEE 802.1x Authentication

These are the IEEE 802.1x authentication limitations:

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

  Use one of these workarounds (CSCsd90495):

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

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

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

  Use one of these workarounds (CSCse04534):

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

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

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

Multicasting

These are the multicasting limitations:

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

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

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

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

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

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

PoE

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

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

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

  There is no workaround. (CSCsg20629)

QoS

These are the quality of service (QoS) limitations:

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

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

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

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

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

RADIUS

- RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN.

  There is no workaround. (CSCta05071)

Routing

These are the routing limitations:

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

  The workaround is to reduce the number of OSPF neighbors to 200 or less. (CSCse65252)
- When the PBR is enabled and QoS is enabled with DSCP settings, the CPU utilization might be high if traffic is sent to unknown destinations.

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

Stacking (only Catalyst 3750-E Switch Stack)

These are the Catalyst 3750-E switch stack limitations:

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

  The workaround is to wait a few seconds and then to reenter the **write memory** privileged EXEC command. (CSCsd66272)
- When using the **logging console** global configuration command, low-level messages appear on both the stack master and the stack member consoles.

  The workaround is to use the **logging monitor** global configuration command to set the severity level to block the low-level messages on the stack member consoles. (CSCsd79037)
- In a mixed stack which consists of Catalyst 3750 switches along with Catalyst 3750-E switches, when the stack ring is congested with approximately 40 Gb/s of traffic, some of the local traffic from one port to another on a Catalyst 3750-E member might be dropped.

  The workaround is to avoid traffic congestion on the stack ring. (CSCsd87538)
- If a new member switch joins a switch stack within 30 seconds of a command to copy the switch configuration to the running configuration of the stack master, the new member might not get the latest running configuration and might not operate properly.

  The workaround is to reboot the new member switch. Use the **remote command all show run** privileged EXEC command to compare the running configurations of the stack members. (CSCsf31301)
- When the flash memory of a stack member is almost full, it might take longer to start up than other member switches. This might cause that switch to miss the stack-master election window. As a result, the switch might fail to become the stack master even though it has the highest priority.

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

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

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

- 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)

SPAN and RSPAN

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

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

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

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

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

VLANs

These are the VLAN limitations:

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

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

- The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:
  - IEEE 802.1 is enabled.
  - A supplicant is authenticated on at least one port.
  - A new member joins a switch stack.

  You can use one of these workarounds:
  - Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.
  - Remove and reconfigure the VLAN. (CSCsi26444)
- 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)

Device Manager Limitations

This is the device manager limitation:

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

  The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

Important Notes

These sections describe the important notes related to this software release for the Catalyst 3750-E and 3560-E switches:

- "Switch Stack Notes" section on page 25
- "Cisco IOS Notes" section on page 26
- "Device Manager Notes" section on page 26

Switch Stack Notes

These notes apply to switch stacks:

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

Cisco IOS Notes

These notes apply to Cisco IOS software:

- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

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

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

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

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

Device Manager Notes

These notes apply to the device manager:

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese.
- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

  From Microsoft Internet Explorer:

  1. Choose **Tools > Internet Options**.
  2. Click **Settings** in the “Temporary Internet files” area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.

- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

  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 severity 3 Cisco IOS configuration caveats apply to both the Catalyst 3750-E and 3560-E switches:

- CSCsx38711 (Catalyst 3750-E switches)

  When a port is configured for single host mode, and the re-authentication timer value is less than 100, if the access control server (ACS) is configured with a per-user access control list (ACL), multiple changes to the stack master might cause the display of empty access-lists for the port.

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

- CSCsx51098 (Catalyst 3750-E switches)

  If the switch stack software is reloaded while the ACS is unreachable, a port configured with a critical VLAN might become error disabled, and a message similar to the one shown below appears on the switch console:

  ```
  *Mar 3 01:10:13.423: %PM-4-ERR_DISABLE_VP: security-violation error detected on
  Fa8/0/7, vlan 3000.
  ```

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

- CSCsx70643 (Catalyst 3750-E switches)

  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.

- CSCsy85676

  When you configure an ACL and enter the **access-group** interface configuration command to apply it to an interface for web authentication, the output from the **show epm session ip-address** or **show ip access_list interface** *interface-id* privileged EXEC command does not show any web authentication filter ID.

  There is no workaround.

- CSCsz18634

  On a switch running Cisco IOS release 12.2(46)SE, the output of the **show interfaces** privileged EXEC command shows 0 packets for port channel input and output rates.

  The workaround is to reload the switch by entering the **reload** privileged EXEC command.

- CSCsz63465

  When an RPS 2300 redundant power supply is connected to a Catalyst3750-E or 3560-E switch and the switch boots up, these messages might appear:

  ```
  00:01:08: %PLATFORM_ENV-1-RPS_PS_THERMAL_CRITICAL: RPS power supply A temperature has
  reached critical threshold
  00:01:08: %PLATFORM_ENV-1-RPS_PS_THERMAL_CRITICAL: RPS power supply B temperature has
  reached critical threshold
  ```

  The root cause of the problem is that when a switch connected to the RPS 2300 is powered up, voltage changes on the switch to RPS communication bus could cause the RPS to erroneously accept commands as data to be written, which corrupts internal data and causes false alarms.

  The workaround is to reset the RPS by entering this command sequence:

  ```
  Switch# configure terminal
  Enter configuration commands, one per line. End with CNTL/Z.
  Switch(config)# service internal
  Switch(config)# end
  Switch# test rps reset
  Are you sure you want to reset the system? [yes/no]: yes
  Switch# configure terminal
  Switch(config)# no service internal
  ```

- CSCta78468

  When VLAN Membership Policy Server (VMPS) is used to configure dynamic VLAN membership on a Catalyst 3750-E or 3560-E switch, hosts or PCs connected to IP phones are denied access to the network. The IP phone continues to operate correctly on the voice VLAN. This issue does not occur on Catalyst 3560 or 3750 switches.

  The workaround is to manually clear the MAC addresses learned on the interface to force a new VMPS query on the next untagged packet received, which is most likely from the PC. Use the **clear mac address-table dynamic interface** [*interface-id*] privileged EXEC command.

- CSCtb08823

  SNMP requests on the stpxRSTPPortRoleTable object only return information for the stack master.

  There is no workaround.

- CSCtb25230 (Catalyst 3750-E switches)

  When a switch stack is configured with DHCP snooping enabled on the host VLAN, hosts connected to the stack master receive bootp packets, but the a packet might not be forwarded to the end hosts connected to stack member switches. The behavior depends on which interface in the stack received the packet.

  The workaround is to disable DHCP snooping for the affected VLAN.

- CSCtb88425

  If you press the MODE button to enter Express Setup setup mode after the switch has received an IP address dynamically through DHCP, HTTP authentication with the default username and password *cisco*/*cisco* fails.

  Use one of these workarounds:

  – Downgrade the image to 12.2(46)SE where there is no HTTP authentication.

  – Use the console to perform initial configuration.

- CSCtc02635

  On switches running Cisco IOS release 12.2(50)SE3 running MAC authentication bypass with multidomain authentication (MDA, IP phones connected to a port might not be able to regain network connectivity in the VOICE domain if the session times out and all RADIUS servers are unreachable.

  There is no workaround.

- CSCtc53453 (Catalyst 3750-E switches)

  If you configure EnergyWise on a member switch and then restart it by entering the **reload slot** *stack-member-number* privileged EXEC command, the EnergyWise configuration is removed from the switch.

  The workaround is to save the switch configuration by using the **copy running-configuration startup-configuration** privileged EXEC command and then restart the switch stack.

Resolved Caveats

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(52)EX1

- CSCtd47552

  The switch fails when you use Cisco License Manager 3.0 to transfer software licenses between switches.

  The workaround is to use the CLI commands to transfer software licenses.

- CSCte44168 (EtherSwitch service modules)

  The call in-progress feature, referred to as activity check, does not work.

  There is no workaround.

- CSCte72452 (EtherSwitch service modules)

  The show energywise neighbors command output is incorrect.

  There is no workaround.

- CSCte96453 (EtherSwitch service modules)

  After you use the energywise level 10 interface configuration command to power on a PoE port, the switch can fail while you configure EnergyWise.

  There is no workaround.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(52)SE and Cisco IOS Release 12.2(52)EX

- CSCsw68528

  On switches running Cisco IOS Release 12.2(44)SE or 12.2(46)SE, when you enter the **show mvr interface** *interface-id* **members** privileged EXEC command to see status of an MVR port, an MVR member port that is not connected always shows as *ACTIVE*.

  The workaround is to use the **show mvr interface** *interface-id* or the **show mvr members** privileged EXEC command. These command outputs show the correct status of an MVR port.

- CSCsw69006 (Catalyst 3750-E switches)

  The **show mvr members** privileged EXEC command output does not include STATIC INACTIVE members. When a static port becomes ACTIVE, it appears in the output as expected.

  There is no workaround.

- CSCsw69015

  When you enter the **mvr vlan** *vlan-id* global configuration command to create an MVR VLAN and enable MVR on the switch by entering the **mvr** global configuration command, if you enter the **show mvr interface** *interface-id* **members** privileged EXEC command, the output shows the MVR groups on the interface. However, if you enable MVR first and then create the MVR VLAN, the MVR groups are not displayed correctly.

  The workaround, if the groups are not displaying correctly, is to create the MVR VLAN *before* enabling MVR. The configuration then displays correctly.

- CSCsw69335 (Catalyst 3750-E switches)

  In a stacked environment, IP ACLs are not applied to interfaces on member switches unless IP routing is enabled.

  The workaround when applying IP ACLs to stack member interfaces is to enable IP routing on the stack master by entering the **ip routing** global configuration command.

- CSCsw96933 (Catalyst 3750-E switches)

  A switch running Cisco IOS Release 12.2(46)SE might lose packets for up to 30 seconds when a link fails. This occurs in some multiple spanning-tree (MST) topologies.

  There is no workaround.

- CSCsw72527

  When a switch sends an ARP request to find the MAC address of the default gateway, the switch sends the request in the wrong VLAN. An ARP entry associating the MAC address with the wrong VLAN is added to the table.

  The workaround is to use the no **arp arpa** global configuration command in all VLANs with IDs lower than the ID of the correct VLAN.

- CSCsx71632

  When VLAN-based quality of service (QoS) is enabled and then disabled on an interface by entering the **mls qos vlan-based** interface configuration command followed by the **no** version of the command, the port policy is not applied properly and could result in undefined behavior for packets matching the port policy.

  The workaround is to remove the port policy by entering the **no service-policy input** *policy-map-name* interface configuration command and then reapply it to the interface.

- CSCsx78068

  If you enable 802.1Q native VLAN tagging by entering the **vlan dot1q tag native** global configuration command and then change the native VLAN ID on an ingress trunk port by entering the sw**itchport trunk native vlan** *vlan-id* interface command, untagged traffic is forwarded instead of being dropped.

  The workaround is to use one of these methods:

  – Enter a **shutdown** followed by a **no shutdown** interface configuration command on the trunk port.

  – Disable and then reenable native VLAN tagging by entering the **no vlan dot1q tag native** global configuration command followed by the **vlan dot1q tag native** command.

- CSCsy90265

  If you repeatedly enter the **show tech-support** privileged EXEC command, the switch might leak memory and, in some cases, shut down.

  The workaround is to reload the switch to clear the memory after repeated use of the **show tech-support** command.

- CSCsz66428

  When flow control is enabled on a port-channel interface and you enter the **flowcontrol receive on** interface configuration command, the bundle is not enabled after the switch restarts. The command appears in the port-channel interface running configuration but does not appear in the switch running configuration. A message such as this appears:

  ```
  %EC-5-CANNOT_BUNDLE2: Gi0/27 is not compatible with Po1 and will be suspended (flow
  control receive of Gi0/27 is on, Po1 is off)
  %EC-5-CANNOT_BUNDLE2: Gi0/28 is not compatible with Po1 and will be suspended (flow
  control receive of Gi0/28 is on, Po1 is off)
  ```

  Use one of these workarounds:

  – To manually configure the port-channel interface, enter the **flowcontrol receive on** interface configuration command.

  – To add the flow-control configuration to the interface after the switch restarts, use an EEM script similar to this:

  ```
  event manager applet Add_flowcontrol_on_restart
  event syslog pattern SYS-5-RESTART
  action 1 cli command "en"
  action 2 cli command "conf t"
  ```

```
action 3 cli command "inter port 1"
action 4 cli command "flowcontrol receive on"
```

For *action 3*, specify the port-channel interface.

- CSCsz72234

  In a VPN routing/forwarding (VRF) instance, a port channel is configured, and the default route is in the global routing table. If a link shuts down while the other links remain up, the port channel might not forward traffic.

  Use one of these workarounds:

  – Enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface command.

  – In the VRF instance, configure the links in the port channel as Layer 2 access links, and configure a switch virtual interface (SVI).

- CSCsz88857 (Catalyst 3750-E switches)

  When an interface on the stack master is a member of an EtherChannel and the channel group number is removed before a master switch changeover, you can not use the same group number when you recreate the EtherChannel after the changeover.

  These are possible workarounds:

  – Reload the switches in the EtherChannel into the channel group that you were not able to create.

  – Use a new channel group number to bundle the physical interfaces in an EtherChannel.

  – Reconfigure the EtherChannel before the master switch changeover.

- CSCta53893

  If the host is in multiple-authentication (multiauth) mode and you configure the fallback authentication process as IEEE 802.1x or MAc authentication bypass, the per-user ACL does not work when the port uses web authentication as the fallback method and then uses 802.1x or MAC authentication bypass as the fallback method.

  The workaround is to restart the switch.

- CSCta57846

  The switch unexpectedly reloads when copying a configuration file from a remote server or from flash memory containing logging file flash:

  The workaround is to enter the **logging file flash**:*filename* global configuration command to configure logging to flash instead of copying to flash.

- CSCta62382

  If an edge switch has this IEEE 802.1Q tunneling configuration:

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport trunk encapsulation dot1q
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
 no cdp enable
```

  The tunnel port might drop IGMP membership reports from hosts. Multicast traffic is not forwarded between customer sites.

  There is no workaround.

- CSCta78502

  When you have configured a login banner by entering the **banner login** *c message c* global configuration command and the switch reloads, the output of banner is missing a carriage return, making the format incorrect.

  There is no workaround.

- CSCta80514

  When you enable MAC address learning on a VLAN and then change the interface configuration (such as adding the VLAN to the list of VLANs allowed on a trunk), MAC address learning is not disabled on the interface. If you disable MAC address learning on the switch, high CPU utilization occurs when the local forwarding manager tries to ut does not learn MAC addresses.

  There is no workaround.

- CSCtb55994

  When EnergyWise Phase 1 is enabled on a switch that has unconnected interfaces, a memory leak might occur over several days.To verify this, use the **show process memory sorted holding | i energy wise** privileged EXEC command.

  The workaround is to disable EnergyWise on the switch.

- CSCtb77378

  When you use IEEE 802.1x authentication with web authentication and an HTTP page opens, the switch redirects the user to an HTTP login page, not a HTTPS login page.

  The workaround is to remove the custom banner.

- CSCtb84303 (Catalyst 3750-E switches)

  In a switch stack, when the SNMP vlan change (vmMembershipEntry) MIB is sent to a member switch other than the stack master, line protocol and notification flapping occurs.

  There is no workaround.

- CSCtb97439

  When remote neighbors change, the LLDP MIB does not properly update the remote neighbors.

  The workaround is to clear the LLDP table by entering the **clear lldp table** privileged EXEC command.

Documentation Updates

These sections provide updates to the product documentation:

- "Update to the Software Configuration Guide" section on page 34
- "Correction to the Software Configuration Guide" section on page 34
- "Updates to the Cisco Software Activation and Compatibility Document" section on page 34
- "Updates to the System Message Guide" section on page 35
- "Update to the Getting Started Guides" section on page 42

Update to the Software Configuration Guide

This section was added to the "Configuring IEEE 802.1x Port-Based Authentication" chapter:

Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the **show authentication** command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

Correction to the Software Configuration Guide

There is no longer a restriction of eight authentications per port, as described in the “Multiple Authentication Mode” section of the “Configuring 802.1x-Based Port Authentication” chapter:

Note Multiple-authentication mode is limited to eight authentications (hosts) per port.

Updates to the 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.

- 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

This section contains the system message guide updates.

New System Messages

These messages were added to the system message guide:

Error Message `DOT1X-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]`

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

Recommended Action No action is required.

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action. AuditSessionID [chars]`

Explanation The system memory is not sufficient to perform the IEEE 802.1x authentication. [chars] is the session ID.

Recommended Action Reduce other system activity to reduce memory demands.

Error Message `DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]`

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

Recommended Action No action is required.

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

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

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

Note This messages applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_PRIMARY_VLAN: Attempt to assign primary VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a primary VLAN to an IEEE 802.1x port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Use a different VLAN.

Note This messages applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_SEC_VLAN: Attempt to assign invalid secondary VLAN [dec] to PVLAN host 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a nonsecondary VLAN to a private VLAN host IEEE 802.1x port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the mode of the port so that it is no longer a PVLAN host port or use a valid secondary VLAN.

Note This messages applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a private VLAN whose primary VLAN does not exist or is shut down. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Make sure the primary VLAN exists and is not shut down. Verify that the private VLAN is associated with a primary VLAN.

Note This messages applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a secondary VLAN to a port that is not a private VLAN host port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the mode of the port so that it is configured as a private VLAN host port, or use a different VLAN that is not configured as a secondary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to an IEEE 802.1x port that is configured as a Switched Port Analyzer (SPAN) destination port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the SPAN configuration so that the port is no longer a SPAN destination port, or change the configuration so that no VLAN is assigned.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_MDA_INACTIVE: Multi-Domain Authentication cannot activate because Data and Voice VLANs are the same on port AuditSessionID [chars]`

Explanation Multi-Domain Authentication (MDA) host mode cannot start if the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port session ID.

Recommended Action Change either the voice VLAN or the access VLAN on the interface so that they are not the same. MDA then starts.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN AuditSessionID [chars]`

Explanation An attempt was made to assign a data VLAN to an IEEE 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change either the voice VLAN or the IEEE 802.1x-assigned VLAN on the interface so that they are not the same.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INTERNAL: Attempt to assign internal VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is used internally and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Explanation Assign a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INVALID: Attempt to assign invalid VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is out of range. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Update the configuration to use a valid VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN [chars] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to an IEEE 802.1x port, but the VLAN was not found in the VLAN Trunking Protocol (VTP) database. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Make sure the VLAN exists and is not shutdown or use another VLAN.

Deleted System Messages

These messages were deleted from the system message guide:

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action.`

Explanation The system memory is not sufficient to perform the IEEE 802.1x authentication.

Recommended Action Reduce other system activity to reduce memory demands.

Error Message `DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars]`

Explanation Authentication was successful. [chars] is the interface.

Recommended Action No action is required.

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

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

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

Note This messages applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_PRIMARY_VLAN: Attempt to assign primary VLAN [dec] to 802.1x port [chars]`

Explanation An attempt was made to assign a primary VLAN to an IEEE 802.1x port, which is not allowed. [dec] is the VLAN, and [chars] is the port.

Recommended Action Use a different VLAN.

Note This messages applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_SEC_VLAN: Attempt to assign invalid secondary VLAN [dec] to PVLAN host 802.1x port [chars]`

Explanation An attempt was made to assign a nonsecondary VLAN to a private VLAN host IEEE 802.1x port. [dec] is the VLAN, and [chars] is the port.

Recommended Action Change the mode of the port so that it is no longer a private VLAN host port, or use a valid secondary VLAN.

Note This messages applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars]`

Explanation An attempt was made to assign a private VLAN whose primary VLAN does not exist or is shut down. [dec] is the VLAN, and [chars] is the port.

Recommended Action Make sure the primary VLAN exists and is not shut down. Verify that the private VLAN is associated with a primary VLAN.

Note This messages applies to switches running the IP base image.

Error Message `DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars]`

Explanation An attempt was made to assign a secondary VLAN to a port that is not a private VLAN host port, which is not allowed. [dec] is the VLAN, and [chars] is the port.

Recommended Action Change the mode of the port so that it is configured as a private VLAN host port, or use a different VLAN that is not configured as a secondary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination`

Explanation An attempt was made to assign a VLAN to an IEEE 802.1x port that is configured as a Switched Port Analyzer (SPAN) destination port. [dec] is the VLAN, and [chars] is the port.

Recommended Action Change the SPAN configuration so that the port is no longer a SPAN destination port, or change the configuration so that no VLAN is assigned.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_MDA_INACTIVE: Multi-Domain Authentication cannot activate because Data and Voice VLANs are the same on port [chars]`

Recommended Action Multi-Domain Authentication (MDA) host mode cannot start if the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port.

Recommended Action Change either the voice VLAN or the access VLAN on the interface so that they are not the same. MDA then starts.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN.`

Explanation An attempt was made to assign a data VLAN to an IEEE 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, and [chars] is the port.

Recommended Action Change either the voice VLAN or the IEEE 802.1x-assigned VLAN on the interface so that they are not the same.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INTERNAL: Attempt to assign internal VLAN [dec] to 802.1x port [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is used internally and cannot be assigned to this port. [dec] is the VLAN, and [chars] is the port.

Recommended Action Assign a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INVALID: Attempt to assign invalid VLAN [dec] to 802.1x port [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is out of range. [dec] is the VLAN, and [chars] is the port.

Recommended Action Update the configuration to use a valid VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN [dec] to 802.1x port [chars]`

Explanation An attempt was made to assign a VLAN to an IEEE 802.1x port, but the VLAN was not found in the VLAN Trunking Protocol (VTP) database. [dec] is the VLAN, and [chars] is the port.

Recommended Action Make sure that the VLAN exists and is not shut down, or use another VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_ON_ROUTED_PORT: Dot1x cannot assign a VLAN [dec] to a routed port [chars]`

Explanation An attempt was made to assign a VLAN to a supplicant on a routed port, which is not allowed. [dec] is the VLAN ID and [chars] is the port.

Recommended Action Either disable the VLAN assignment, or change the port type to a nonrouted port.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_PROMISC_PORT: Attempt to assign VLAN [dec] to promiscuous 802.1x port [chars]`

Explanation An attempt was made to assign a VLAN to a promiscuous IEEE 802.1x port, which is not allowed. [dec] is the VLAN, and [chars] is the port.

Recommended Action Change the port mode so that it is no longer a promiscuous port, or change the configuration so that no VLAN is assigned.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_RESERVED: Attempt to assign reserved VLAN [dec] to 802.1x port [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is a reserved VLAN and cannot be assigned to this port. [dec] is the VLAN, and [chars] is the port.

Recommended Action Assign a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_RSPAN: Attempt to assign RSPAN VLAN [dec] to 802.1x port [chars]. 802.1x is incompatible with RSPAN`

Explanation This message means that remote SPAN should not be enabled on a VLAN with IEEE 802.1x-enabled. [dec] is the VLAN, and [chars] is the port.

Recommended Action Either disable remote SPAN configuration on the VLAN, or disable IEEE 802.1x on all the ports in this VLAN.

Update to the 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

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

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

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

These documents provide complete information about the switches:

- Catalyst 3750-E Switch Getting Started Guide
- Catalyst 3560-E Switch Getting Started Guide
- *Catalyst 3750-E and Catalyst 3560-E Switch Hardware Installation Guide*
- Regulatory Compliance and Safety Information for the Catalyst 3750-E and *Catalyst* 3560-E Switch
- *Release Notes for the Catalyst 3750-E and Catalyst 3560-E Switch*
- *Catalyst 3750-E and Catalyst 3560-E Switch Software Configuration Guide*
- *Catalyst 3750-E and Catalyst 3560-E Switch Command Reference*
- *Catalyst 3750-E and Catalyst 3560-E Switch System Message Guide*
- *Cisco Software Activation and Compatibility Document*

- *Installation Notes for the Catalyst 3750-E, Catalyst 3560-E Switches, and RPS 2300 Power Supply Modules*
- *Installation Notes for the Catalyst 3750-E and Catalyst 3560-E Switch Fan Module*
- *Installation Notes for the Cisco TwinGig Converter Module*
- *Cisco Redundant Power System 2300 Hardware Installation Guide*
- *Cisco Redundant Power System 2300 Compatibility Matrix*
- Device manager online help (available on the switch)

These compatibility matrix documents are available from this Cisco.com site:

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

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

For other information about related products, see these documents:

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

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

- *Connecting Cisco Enhanced EtherSwitch Service Modules to the Network* at

  http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/eesm_hw.html
- *Cisco Enhanced EtherSwitch Service Modules Configuration Guide* at

  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, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation and Submitting a Service Request" section.