



# Release Notes for the Catalyst 2960-S, 2960-SF, 2960-C, 2960-Plus, and 3560-C Switches, Cisco IOS Release 15.2(1)E and Later

---

March 12, 2014

Cisco IOS Release 15.2(1)E and later runs on Catalyst 2960-S, 2960-SF, 2960-C, 2960-Plus and 3560-C switches and on Cisco EtherSwitch service modules.

The Catalyst 2960-S supports switch stacking. Unless otherwise noted, the term *switch* refers to a standalone switch and not to a switch stack.

The Catalyst 3560-C switch does not support the IP services image.

These release notes include important information about Cisco IOS Release 15.2(1)E and any limitations, restrictions, and caveats that apply to the releases. 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 5.
- 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 5.

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

## Contents

- [System Requirements](#), page 2
- [Upgrading the Switch Software](#), page 4
- [Installation Notes](#), page 7
- [New Software Features](#), page 8
- [Minimum Cisco IOS Release for Major Features](#), page 10



---

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

© 2013 Cisco Systems, Inc. All rights reserved.

- [Limitations and Restrictions, page 11](#)
- [Important Notes, page 17](#)
- [Open Caveats, page 19](#)
- [Resolved Caveats, page 20](#)
- [Obtaining Documentation and Submitting a Service Request, page 25](#)

## System Requirements

- [Supported Hardware, page 2](#)
- [Device Manager System Requirements, page 3](#)
- [Cluster Compatibility, page 4](#)
- [CNA Compatibility, page 4](#)

## Supported Hardware

**Table 1** *Catalyst 2960-S and 2960-P Switches Supported*

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960S-48FPD-L <sup>1</sup>	48 10/100/1000 Power over Ethernet Plus (PoE+) ports (PoE budget of 740 W) and 2 SFP+ <sup>2</sup> module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48LPD-L <sup>1</sup>	48 10/100/1000 PoE+ ports (PoE budget of 370 W) and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24PD-L <sup>1</sup>	24 10/100/1000 PoE+ ports (PoE budget of 370 W) and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TD-L <sup>1</sup>	48 10/100/1000 ports and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TD-L <sup>1</sup>	24 10/100/1000 ports and 2 SFP+ module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48FPS-L <sup>1</sup>	48 10/100/1000 PoE+ ports (PoE budget of 740 W) and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48LPS-L <sup>1</sup>	48 10/100/1000 PoE+ ports (PoE budget of 370 W) and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24PS-L <sup>1</sup>	24 10/100/1000 PoE+ ports (PoE budget of 370 W) and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TS-L <sup>1</sup>	48 10/100/1000 ports and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TS-L <sup>1</sup>	24 10/100/1000 ports and 4 SFP module slots	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-F48FPS-L <sup>1</sup>	48 10/100 PoE+ ports (PoE budget of 740 W) and 4 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F48LPS-L <sup>1</sup>	48 10/100 PoE+ ports (PoE budget of 370 W) and 4 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F48TS-L <sup>1</sup>	48 10/100 ports and 4 SFP module slots	Cisco IOS Release 15.0(2)SE

**Table 1** Catalyst 2960-S and 2960-P Switches Supported (continued)

Switch	Description	Supported by Minimum Cisco IOS Release
Catalyst 2960S-F24PS-L <sup>1</sup>	24 10/100 PoE+ ports (PoE budget of 370 W) and 2 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F24TS-L <sup>1</sup>	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F48TS-S	48 10/100 ports and 2 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F24TS-S	24 10/100 ports and 2 SFP module slots	Cisco IOS Release 15.0(2)SE
Catalyst C2960P-48PST-L	48 10/100 ports with PoE, 2 1000BASE-T and 2 SFP uplinks, LAN Base image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24PC-L	24 10/100 ports with PoE, 2 1000BASE-T or SFP uplinks, LAN Base image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24LC-L	24 10/100 ports, 8 ports with PoE, 2 1000BASE-T or SFP uplinks, LAN Base image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-48TC-L	48 10/100 ports, 2 1000BASE-T or SFP uplinks, LAN Base image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24TC-L	24 10/100 ports, 2 1000BASE-T or SFP uplinks, LAN Base image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-48PST-S	48 10/100 ports with PoE, 2 1000BASE-T and 2 SFP uplinks, LAN Lite image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24PC-S	24 10/100 ports with PoE, 2 1000BASE-T or SFP uplinks, LAN Lite image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24LC-S	24 10/100 ports, 8 ports with PoE, 2 1000BASE-T or SFP uplinks, LAN Lite image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-48TC-S	48 10/100 ports, 2 1000BASE-T or SFP uplinks, LAN Lite image	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24TC-S	24 10/100 ports, 2 1000BASE-T or SFP uplinks, LAN Lite image	Cisco IOS Release 15.0(2)EZ

1.Support Cisco FlexStack technology.

2.SFP+ = 10 Gigabit fiber uplink.

## Device Manager System Requirements

- [Hardware Requirements, page 3](#)
- [Software Requirements, page 4](#)

## Hardware Requirements

**Table 2** Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum <sup>1</sup>	512 MB <sup>2</sup>	256	1024 x 768	Small

1. We recommend 1 GHz.

2. We recommend 1 GB DRAM.

## Software Requirements

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 6.0 or 7.0, and Firefox up to version 27, with JavaScript enabled.

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

## Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI) or the Network Assistant application.

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 2960-C switch, all standby command switches must be Catalyst 2960-C switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant* and *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com), the software configuration guide, the command reference, and the Cisco EtherSwitch service module feature guide.

## CNA Compatibility

Cisco IOS 12.2(50)SE and later is only compatible with Cisco Network Assistant (CNA) 5.0 and later. You can download Cisco Network Assistant from this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/NetworkAssistant>

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

## Upgrading the Switch Software

- [Finding the Software Version and Feature Set, page 5](#)
- [Deciding Which Files to Use, page 5](#)
- [Archiving Software Images, page 5](#)
- [Upgrading a Switch by Using the Device Manager or Network Assistant, page 6](#)
- [Upgrading a Switch by Using the CLI, page 6](#)
- [Recovering from a Software Failure, page 7](#)

## 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.

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
c3560c405ex-universalk9npe-tar.152-1.E.tar	Catalyst 3560-C image with all supported universal image features and Web-based device manager, does not support MACsec encryption.
c3560c405ex-universalk9-tar.152-1.E.tar	Catalyst 3560-C image with all supported universal image features and Web-based device manager.
c3560c405-universalk9npe-tar.152-1.E.tar	Catalyst 3560-C image with all supported universal image features and Web-based device manager, does not support MACsec encryption.
c3560c405-universalk9-tar.152-1.E.tar	Catalyst 3560-C image with all supported universal image features and Web-based device manager.
c2960s-universalk9-tar.152-1.E.tar	LAN Base and LAN Lite crypto image with device manager
c2960c405ex-universalk9-tar.152-1.E.tar	Catalyst 2960-C image with all supported universal image features and Web-based device manager.
c2960c405-universalk9-tar.152-1.E.tar	Catalyst 2960-C image with all supported universal image features and Web-based device manager.

## 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 to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

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

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod\\_bulletin0900aecd80281c0e.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html)

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



**Note**

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

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

[http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf\\_t1.html](http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html)

## Upgrading a Switch by Using the Device Manager or Network Assistant

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



**Note**

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

## Upgrading a Switch by Using the CLI

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

To download software, follow these steps:

**Step 1** Use [Table 3 on page 5](#) to identify the file that you want to download.

**Step 2** Download the software image file:

- a. If you are a registered customer, go to this URL and log in.  
<http://www.cisco.com/cisco/web/download/index.html>
- b. Navigate to **Switches > LAN Switches - Access**.
- c. Navigate to your switch model.
- d. Click **IOS Software**, then select the latest IOS release.

Download the image you identified in [Step 1](#).

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

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

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

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

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

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

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

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

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

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

The **/allow-feature-upgrade** option allows installation of an image with a different feature set (for example, upgrade from the IP base image to the IP services image).

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/c3750-ipservices-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 recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

## Installation Notes

Use these methods to assign IP information to your switch:

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

# New Software Features

## New in Cisco IOS Release 15.2(1)E

- (Catalyst Switches 2960-C LAN Base, 3560-C LAN Base) The First Hop Security feature in IPv6 supports the Router Advertisement guard which analyzes the RAs and filters out bogus RAs sent by unauthorized routers.
- (Catalyst Switches 2960-C LAN Base, 3560-C LAN Base) The First Hop Security feature also supports Binding Integrity Guard. Binding integrity guard uses the Binding table to ensure that rogue users cannot steal or spoof addresses.
- (Catalyst switch 2960-Plus) The First Hop Security feature in IPv6 supports the Router Advertisement guard which analyzes the RAs and filters out bogus RAs sent by unauthorized routers.
- (Catalyst Switches 2960-S, 2960-SF and 2960-C, and 3560-C LAN Base) Support for IPv6 QoS.
- (LAN Base) Support for ciscoDynamicArpInspectionMIB.
- (Catalyst Switches 2960-S, 2960-SF, and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) Support for Smart Install Upgrade Fallback, configuration-only deployment, and image-only upgrade.
- (Catalyst Switches 2960-S, 2960-SF and 3560-C LAN Base) Support for Hop by Hop EH ACL Throttling and Filtering.
- (Catalyst Switches 2960-S, 2960-SF and 2960-C LAN Lite; 3560-C LAN Base) Support for GLC-T SFP+ ports.
- (Catalyst Switches 2960-S, 2960-SF and 2960-C LAN Lite; 3560-C LAN Base) Support for GLC-GE-100FX on SFP+ ports.(Not supported on Wall-E)
- (Catalyst Switches 2960-S, 2960-SF, and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) Support for script based zero touch provisioning.
- (Catalyst Switches 2960-S and 2960-SF LAN Base) Support for DWDM SFP+.
- (Catalyst Switches 2960-S and 2960-SF LAN Base) Support for SFP+ ZR.
- (Catalyst Switches 2960-S, 2960-SF, and 2960-C LAN Lite) The Digital Optical Monitoring (DOM) MIB for SFP optical transceivers allows you to monitor real-time operating parameters. Each DOM-capable optical transceiver has five sensors that are configured to monitor operational parameters such as temperature, voltage, laser bias current, and optical TX and Rx power on a specific interface.
- (Catalyst Switch 3560-C IP Base) Support for MSP and metadata.
- (Catalyst Switch 3560-C IP Base) Supports manually configured tunneling over IPv4.
- (Catalyst Switch 3560-C IP Base) Support for IPv6 EIGRP stub routing.
- (Catalyst Switch 3560-C IP Base) Support for IPv6 PIM stub routing.
- (Catalyst Switches 2960-S and 2960-SF LAN Base) Support for SXP loop detection.
- (Catalyst Switches 2960-S, 2960-SF, 2960-C, and 3560-C IP Base; 2960-Plus LAN Base) Support for DHCP glean for device sensor.
- (Catalyst Switch 3560-C IP Base) Support for encrypting PMK password inside the switch.
- (LAN Base) Support for CISCO-EMBEDDED-EVENT-MGR-MIB.



- (Catalyst Switches 2960-S, 2960-SF, and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) Support for SNMP-COMMUNITY-MIB.
- IPv6 Compliant Features:
  - (Catalyst Switches 2960-S, 2960-SF, and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) Updated ICMP RFCs 4291, 4443, 3484, 2526, 4861, 4862, 5095, 4007, 3513.
  - (Catalyst Switch 2960-S, 2960-SF, and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) Support for UDP MIB (RFC 4113) and TCP MIB (RFC 4022).
- (Catalyst Switch 3560-C IP Base) EIGRP features:
  - EIGRP IPv6 NSF/GR
  - EIGRP MIB
  - EIGRP IPv6 MIBs
  - Route Tag Enhancements
  - Generate SNMP trap when EIGRP neighbor is down
  - Disable IPX in EIGRP
  - EIGRP add-path
  - Support for EIGRP wide metrics
- (Catalyst Switch 3560-C IP Base) OSPF features:
  - OSPFv3 BFD
  - OSPFv3 Graceful Shutdown
  - OSPFv2 NSSA
  - OSPFv3 NSSA Option
  - OSPFv3 External Path Preference
  - OSPFv3 Router Max metric Router LSA
  - OSPFv3 Retransmission Limit
  - Support for OSPFv3 Prefix Suppression
  - Support for OSPFv3 Area Filter/DC Ignore
  - OSPFv3 MIB, OSPF MIB
- (Catalyst Switches 2960-S, 2960-SF, and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) IPv6 support for TFTP
- (Catalyst Switches 2960-S, 2960-SF and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) Support for DNS over IPv6
- (Catalyst Switch 3560-C IP Base) Support for HSRP-aware PIM.
- (LAN Base) IPv6 Neighbor Discovery enhancements:
  - Enhancement to create global IPv6 entries for unsolicited NA
  - IPv6 ND cache expire
  - Option to configure exponential backoff for NS timer used in NUD
- (IP Services) BGP Features:
  - Support for 4 byte BGP ASN numbers
  - BGP support for malformed attribute error handling

- BGP support for Cisco-BGP-MIBv2
- BGP support for graceful shutdown
- BGP support for Add-Path
- BGP support for VRF dynamic route leaking (for VRF lite)



**Note**

The Catalyst 3560-C switch does not support BGP.

- (Catalyst Switches 2960-S, 2960-SF, and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) Support for Netconf XML PI **show output**
- (Catalyst Switches 2960-S, 2960-SF, and 2960-C LAN Lite; 2960-Plus and 3560-C LAN Base) Configurable TCP Keep Alive timer

## Minimum Cisco IOS Release for Major Features

Table 4 lists the minimum software release required to support the major features of the Catalyst 2960-S, 2960-C, and 3560-C switches and the Cisco EtherSwitch service modules.

**Table 4** Catalyst 2960-S, 2960-C, and 3560-C Switches and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Cisco TrustSec SXP version 2, syslog messages, and SNMP support	15.0(2)SE	3560-C, 2960-S, 2960-C
Critical voice VLAN	15.0(1)SE	2960-S
NEAT enhancement to control access to the supplicant port	15.0(1)SE	2960-S
Auto Smartports improved device classification	15.0(1)SE	2960-S
EnergyWise Phase 2.5	12.2(58)SE1	2960-S
Protocol storm protection	12.2(58)SE1	2960-S
Smart Install 3.0	12.2(58)SE1	2960-S
Auto Smartports enhancements to enable auto-QoS on a digital media player.	12.2(58)SE1	2960-S
Memory consistency check routines	12.2(58)SE1	2960-S
Call Home support	12.2(58)SE1	2960-S
NTP version 4	12.2(58)SE1	2960-S
RADIUS, TACACS+, and SSH/SCP over IPv6	12.2(58)SE1	2960-S
IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates	12.2(58)SE1	2960-S
Auto-QoS enhancements	12.2(55)SE	2960-S
Auto Smartport enhancements including global macros	12.2(55)SE	2960-S
Smart Install enhancements and new features	12.2(55)SE	2960-S
Port ACL improvements	12.2(55)SE	2960-S
CDP and LLDP location enhancements	12.2(55)SE	2960-S

**Table 4** *Catalyst 2960-S, 2960-C, and 3560-C Switches and the Minimum Cisco IOS Release Required (continued)*

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Support
Multi-authentication with VLAN assignment	12.2(55)SE	2960-S
Static routing support on SVIs	12.2(55)SE	2960-S
MAC replace to end a session when a host disconnects from a port.	12.2(55)SE	2960-S
DHCP snooping and Option 82 and LLPD-MED in LAN lite image	12.2(55)SE	2960-S

## Limitations and Restrictions

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

- [Cisco IOS Limitations, page 11](#)
- [Device Manager Limitations, page 17](#)

## Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 2960-S, 2960-SF, 2960-C, 2960-Plus, and 3560-C switches:

- [Configuration, page 11](#)
- [Ethernet, page 12](#)
- [HSRP, page 13](#)
- [HSRP, page 13](#)
- [IP, page 13](#)
- [IP Telephony, page 13](#)
- [Power, page 14](#)
- [QoS, page 14](#)
- [Smart Install, page 15](#)
- [SPAN and RSPAN, page 16](#)
- [Spanning Tree Protocol, page 16](#)
- [Trunking, page 16](#)
- [VLAN, page 17](#)

## Configuration

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs if a crypto key is generated after an SSL client session.

There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

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

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

- A ciscoFlashMIBTrap message appears during switch startup. This does not affect switch functionality. (CSCsj46992)

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

The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

- When authorization and accounting are enabled on the switch and you use the interface range command to change the configuration on a range of interfaces, the change might cause high CPU utilization and authentication failures.

The workaround is to disable authorization and accounting or to enter the configuration change for one interface at a time. (CSCsg80238, CSCti76748)

## Ethernet

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

If this happens, uneven traffic distribution will happen on EtherChannel ports.

Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

- for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
- for incrementing source-ip traffic, configure load balance method as **src-ip**
- for incrementing dest-ip traffic, configure load balance method as **dst-ip**
- Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

## HSRP

- When the active switch fails in a switch cluster that uses HSRP redundancy, the new active switch might not contain a full cluster member list.

The workaround is to ensure that the ports on the standby cluster members are not in the spanning-tree blocking state. To verify that these ports are not in the blocking state, see the “Configuring STP” chapter in the software configuration guide. (CSCec76893)

## IP

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console.

The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

## IP Telephony

- After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned.

No workaround is necessary. (CSCea85312)

- Some access point devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These access points should be discovered as Cisco pre-standard devices. The **show power inline** user EXEC command shows the access point as an IEEE Class 1 device.

The workaround is to power the access point by using an AC wall adaptor. (CSCin69533)

- The Cisco 7905 IP Phone is error-disabled when the phone is connected to wall power.

The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise.

The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)

- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port.

There is no workaround. (CSCdy82818)

- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:

- If the ALLOW\_NEW\_SOURCE record is before the BLOCK\_OLD\_SOURCE record, the switch removes the port from the group.
- If the BLOCK\_OLD\_SOURCE record is before the ALLOW\_NEW\_SOURCE record, the switch adds the port to the group.

There is no workaround. (CSCec20128)

- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

After you configure a switch to join a multicast group by entering the **ip igmp join-group group-address** interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

Use one of these workarounds:

- Cancel membership in the multicast group by using the **no ip igmp join-group group-address** interface configuration command on an SVI.
- Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan vlan-id** global configuration command. (CSCeh90425)

## Power

- Entering the **shutdown** and the **no shutdown** interface configuration commands on the internal link can disrupt the PoE operation. If a new IP phone is added while the internal link is in shutdown state, the IP phone does not get inline power if the internal link is brought up within 5 minutes.

The workaround is to enter the **shutdown** and the **no shutdown** interface configuration commands on the Fast Ethernet interface of a new IP phone that is attached to the service module port after the internal link is brought up. (CSCeh45465)

## QoS

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue.

The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)

- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)
- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

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

There is no impact to switch functionality.

There is no workaround. (CSCtg32101)

## RADIUS

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

## Smart Install

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

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

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

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

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

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

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

Use one of these workarounds:

- If client needs to upgrade using an image and configuration file configured in the DHCP server options, you should remove the client from the Smart Install network during the upgrade.
- In a network using Smart Install, you should not configure options for image and configuration in the DHCP server. For clients to upgrade using Smart Install, you should configure product-id specific image and configuration files in the director. (CSCte99366)
- If the director in the Smart Install network is located between an access point and the DHCP server, the access point tries to use the Smart Install feature to upgrade even though access points are not supported devices. The upgrade fails because the director does not have an image and configuration file for the access point.

There is no workaround. (CSCtg98656)

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

- When you enter any password in the director CLI, the upgrade should not be allowed, but it is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.

There is no workaround. (CSCth35152)

## SPAN and RSPAN

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

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

- CDP, VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session session\_number destination {interface interface-id encapsulation replicate}** global configuration command for local SPAN. (CSCed24036)

## Spanning Tree Protocol

- CSCtl60247

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

There is no workaround.

## Trunking

- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y.

There is no workaround. (CSCdz42909).

- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics.

There is no workaround. (CSCec35100).



## VLAN

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

- When 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)

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

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

## Device Manager Limitations

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

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

## Important Notes

- [Switch Stack Notes, page 17](#)
- [Catalyst 2960-S Control Plane Protection, page 17](#)
- [Catalyst 2960-S Control Plane Protection, page 17](#)
- [Device Manager Notes, page 18](#)

## Switch Stack Notes

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

## Catalyst 2960-S Control Plane Protection

Catalyst 2960-S switches internally support up to 16 different control plane queues. Each queue is dedicated to handling specific protocol packets and is assigned a priority level. For example, STP, routed, and logged packets are sent to three different control plane queues, which are prioritized in corresponding order, with STP having the highest priority. Each queue is allocated a certain amount of processing time based on its priority. The processing-time ratio between low-level functions and high-level functions is allocated as 1-to-2. Therefore, the control plane logic dynamically adjusts the CPU utilization to handle high-level management functions as well as punted traffic (up to the maximum CPU processing capacity). Basic control plane functions, such as the CLI, are not overwhelmed by functions such logging or forwarding of packets.

## Cisco IOS Notes

- 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, check that there is network connectivity between the switch and the ACS. You should also check 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

- 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.
- The Legend on the device manager incorrectly includes the 1000BASE-BX SFP module.
- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

From Microsoft Internet Explorer:

- Choose **Tools > Internet Options**.
  - Click **Settings** in the “Temporary Internet files” area.
  - From the Settings window, choose **Automatically**.
  - Click **OK**.
  - 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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication {aaa   enable   local}</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> <li>• <b>aaa</b>—Enable the authentication, authorization, and accounting feature. You must enter the <b>aaa new-model</b> interface configuration command for the <b>aaa</b> keyword to appear.</li> <li>• <b>enable</b>—Enable password, which is the default method of HTTP server user authentication, is used.</li> <li>• <b>local</b>—Local user database, as defined on the Cisco router or access server, is used.</li> </ul>
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.

The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, `http://10.1.126.45:184` where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, `www.cisco.com:84`), you must enter `http://` as the URL prefix. Otherwise, you cannot launch the device manager.

## Open Caveats

Unless otherwise noted, these caveats apply to the Catalyst 2960-S, 2960-SF, 2960-C, 2960-Plus, and 3560-C switches:

- CSCtq35006

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

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

- CSCtr87645

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

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

- CSCua58659 (Catalyst 2960-S switch)

The global **power inline consumption default 15400** command fails to restrict the power consumption of a PoE+ port 15.4 W.

The workaround is to use the **power inline consumption 15400** command in interface configuration mode.

- CSCug54690

IPv6 access-list counters do not increment when a policymap associated with a classmap that matches an IPv6 ACL is applied to a physical interface and matching traffic is sent.

There is no workaround.

- CSCug69823

System crashes if you remove EnergyWise SNMP proxy configuration immediately after configuring it.

The workaround is to wait for some time after configuring EnergyWise SNMP proxy, and then remove the configuration to avoid a crash.

- CSCug74567 (Catalyst 2960-S and 2960-SF switches)

On reloading the stack master, the supplicants with Filter-ID lose connectivity.

The workaround is to use dACL instead of Filter-ID. For supplicants with Filter-ID, there would be loss of connectivity until a new session is established.

- CSCuj00841 (Catalyst 3560-CG switch)

The Cisco TrustSec feature is not available.

There is no workaround.

- CSCuj35704

A Dynamic ACL with a remark statement is not pushed from ISE to client and authorization either fails or is unauthorized.

The workaround is to remove the remark statement from the DACL.

## Resolved Caveats

- [Caveats Resolved in Cisco IOS Release 15.2\(1\)E2, page 21](#)
- [Caveats Resolved in Cisco IOS Release 15.2\(1\)E1, page 21](#)
- [Caveats Resolved in Cisco IOS Release 15.2\(1\)E, page 22](#)

## Caveats Resolved in Cisco IOS Release 15.2(1)E2

- CSCu190866 (Catalyst 3560-C)  
The switch resets during normal network operation due to a malformed Multicast Domain Name service (mDNS) packet.  
There is no workaround.

## Caveats Resolved in Cisco IOS Release 15.2(1)E1

- CSCts80209  
If **login quiet-mode** is configured, the switch resets when you enter the **no login block-for** command.  
There is no workaround.
- CSCuc53853  
Provided an HTTP server is enabled on a switch, a vulnerability exists in Cisco IOS switches where the remote, non-authenticated attacker can cause Denial of Service (DoS) by reloading an affected device. An attacker can exploit this vulnerability by sending a special combination of crafted packets.  
There is no workaround.
- CSCui65252  
When Dynamic ARP Inspection (DAI) is enabled over port channel, it stops processing the Address Resolution Protocol (ARP) packets.  
The workaround is to set up a direct link between the access switch and the DHCP server.
- CSCuj00841  
Cisco TrustSec (CTS) feature is not supported on the switch.  
There is no workaround.
- CSCuj29803  
Security Group Access Control List (SGACL) with log option set on the switch does not print syslogs.  
There is no workaround.
- CSCuj46750  
Cisco TrustSec Security Group Tag Exchange Protocol (CTS-SXP) is missing on the switch.  
There is no workaround.
- CSCuj56845  
When you enable either the device-sensor accounting or the access-session accounting attributes command, the accounting request is not sent from the switch to the radius (ISE) Server.  
The workaround is to not enable device-sensor accounting. The user accounting message will not carry the device-sensor attributes to the ISE.
- CSCuj87317  
VRRPv3 is not available on the switch in Cisco IOS Release 15.2(1)E.  
VRRPv3 is made available from Cisco IOS Release 15.2(1)E1.

## Caveats Resolved in Cisco IOS Release 15.2(1)E

- CSCua59800 (Catalyst 2960-S switch)
 

If Flex Links is configured on a Catalyst 2960-S switch stack, and the switches in the stack are disconnected from each other (due to a connection problem), the backup port switch sends dummy multicast messages to its peer switches (although its MAC address is not present in the MAC address table).

The workaround is to reload the switch stack.
- CSCua74302 (Switches running the LAN base image)
 

Access Control Lists (ACLs) applied to outbound traffic on the switch virtual interface (SVI) do not work.

There is no workaround.
- CSCuc51915
 

A Preboot Execution Environment (PXE) enabled host is unable to boot properly when IP Source Guard is configured on the switch.

There is no workaround.
- CSCud47137 (Catalyst 2960-S switch)
 

After the master switch failure, the stack member links within an LACP-enabled EtherChannel fails to recover.

The workaround is to restart the switch, which will recover a link failure.
- CSCue09838 (Catalyst 2960-C switch)
 

The VLAN goes down when collecting information from the **show tech-support details** command through Telnet sessions.

The workaround is to reload the switch.
- CSCuf13634
 

The interface status shows that the port is up, and duplex and speed are set to auto, even though link negotiation is disabled (when using the **speed nonegotiate** interface configuration command).

The workaround is to restart the interface using the **shutdown** and **no shutdown** interface configuration command.
- CSCuf77683
 

Internal VLANs are displayed when the **show snmp mib ifmib ifindex** command is entered or the SNMP is queried for the ipMIB object.

The workaround is to check if the displayed VLANs are internal and then to hide them.
- CSCug17582
 

When AAA is configured, the following message is displayed when entering the **enable** command:

```
Password required, but none set
```

The workaround is to enter the **aaa authentication enable default enable** global configuration command.
- CSCug43533
 

If macros are used for device classification, the CISCO\_LAST\_RESORT\_EVENT macro is triggered on the switch inexplicably.

There is no workaround.

- CSCug51225 (Catalyst 2960-S and 2960-C switches)  
If a new member is added to the switch stack, a Topology Change Notification (TCN) flood is triggered on the network.  
There is no workaround.
- CSCug67745 (Catalyst 3560-C switch)  
In multicast mode, Web Cache Communication Protocol (WCCP) ISY packets are not received by the cache engine.  
The workaround is to use unicast mode.
- CSCuh04978 (Catalyst 2960-S switch)  
A MAC address that is learned dynamically on a port is deleted even with continuous incoming traffic. This results in unicast flooding for packets destined to the MAC address that has been deleted.  
The workaround is to configure the MAC address entry statically or to disable the device classifier (using the **no macro auto monitor** global configuration command).
- CSCuh12528  
With DHCP address conflict resolution enabled (by using the **ip dhcp conflict resolution** global configuration command), the switch stops operating when the **clear ip dhcp conflict** command is entered.  
There is no workaround.

## Related Documentation

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

These documents provide more information about the Catalyst 2960-S, 2960-SF, 2960-C, 2960-Plus, and 3560-C switches and are available at Cisco.com:

[http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html)

[http://www.cisco.com/en/US/products/hw/switches/ps5528/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/switches/ps5528/tsd_products_support_series_home.html)

[http://www.cisco.com/en/US/products/ps10081/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps10081/tsd_products_support_series_home.html)

[http://www.cisco.com/en/US/products/ps6406/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html)

These documents provide complete information about the Catalyst 2960 and 2960-S switches and are available on Cisco.com:

- *Catalyst 2960 and 2960-S Switch Software Configuration Guide*
- *Catalyst 2960 and 2960-S Switch Command Reference*
- *Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide*
- *Catalyst 2960-S Switch Hardware Installation Guide*
- *Catalyst 2960-S Switch Getting Started Guide*
- *Catalyst 2960 Switch Hardware Installation Guide*

- *Catalyst 2960 Switch Getting Started Guide*
- *Catalyst 2960 Switch Getting Started Guide*—available in English, simplified Chinese, French, German, Italian, Japanese, and Spanish
- *Regulatory Compliance and Safety Information for the Catalyst 2960 and 2960-S Switch*

For other information about related products, see these documents:

- *Smart Install Configuration Guide*
- *Auto Smartports Configuration Guide*
- *Cisco EnergyWise Configuration Guide*
- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*
- *Cisco RPS 300 Redundant Power System Hardware Installation Guide*
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide*
- For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide*
- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site: [http://www.cisco.com/en/US/products/hw/modules/ps5455/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html)  
SFP compatibility matrix documents are available from this Cisco.com site: [http://www.cisco.com/en/US/products/hw/modules/ps5455/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html)



# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

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

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

---

This document is to be used in conjunction with the documents listed in the “[Obtaining Documentation and Submitting a Service Request](#)” section.

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

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

© 2011–2014 Cisco Systems, Inc. All rights reserved.

