Release Notes for the Catalyst 3750, 3560, 2975, 2960-S, and 2960 Switches, Cisco IOS Release 12.2(55)SE and Later

Revised September 25, 2018

Cisco IOS Release 12.2(55)SE runs on all Catalyst 3750, 3560, 2975, 2960-S, and 2960 switches and on Cisco EtherSwitch service modules.

Cisco IOS Release 12.2(55)SE1 runs on all Catalyst 3750, 3560, 2960-S, and 2960 switches and on Cisco EtherSwitch service modules.

Cisco IOS Release 12.2(55)SE2 runs on Catalyst 2960-S switches only.

The Catalyst 3750 switches and the Cisco EtherSwitch service modules support stacking through Cisco StackWise technology. The Catalyst 3560 and 2960 switches do not support switch stacking. Catalyst 2960-S and 2975 do support stacking. Unless otherwise noted, the term switch refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 12.2(55)SE and later, and any limitations, restrictions, and caveats that apply to 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 7.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “Deciding Which Files to Use” section on page 8.

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

- System Requirements, page 2
- Upgrading the Switch Software, page 7
- Installation Notes, page 11
- New Software Features, page 12
- Minimum Cisco IOS Release for Major Features, page 13
- Limitations and Restrictions, page 19
- Important Notes, page 36
- Open Caveats, page 38
- Resolved Caveats, page 41
- Documentation Updates, page 66
- Obtaining Documentation and Submitting a Service Request, page 87

System Requirements

- Supported Hardware, page 2
- Device Manager System Requirements, page 6
- Cluster Compatibility, page 7
- CNA Compatibility, page 7

Supported Hardware

Table 1   Catalyst 3750 and Cisco EtherSwitch Service Modules Supported

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3750G-24WS-S25</td>
<td>24 10/100/1000 PoE(^1) ports, 2 SFP(^2) module slots, and an integrated wireless LAN controller supporting up to 25 access points.</td>
<td>Cisco IOS Release 12.2(25)FZ or Cisco IOS Release 12.2(35)SE</td>
</tr>
<tr>
<td>Catalyst 3750G-24WS-S50</td>
<td>24 10/100/1000 PoE ports, 2 SFP module slots, and an integrated wireless LAN controller supporting up to 50 access points</td>
<td>Cisco IOS Release 12.2(25)FZ or Cisco IOS Release 12.2(35)SE</td>
</tr>
<tr>
<td>Catalyst 3750-24FS</td>
<td>24 100BASE-FX ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(25)SEB</td>
</tr>
<tr>
<td>Catalyst 3750-24PS</td>
<td>24 10/100 PoE ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3750-24TS</td>
<td>24 10/100 Ethernet ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3750-48PS</td>
<td>48 10/100 PoE ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3750-48TS</td>
<td>48 10/100 Ethernet ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3750G-12S</td>
<td>12 SFP module slots</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
</tbody>
</table>
### Table 1  Catalyst 3750 and Cisco EtherSwitch Service Modules Supported  (continued)

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3750G-16TD</td>
<td>16 10/100/1000 Ethernet ports and 1 XENPAK 10-Gigabit Ethernet module slot</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3750G-24PS</td>
<td>24 10/100/1000 PoE ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3750G-24T</td>
<td>24 10/100/1000 Ethernet ports</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3750G-24TS</td>
<td>24 10/100/1000 Ethernet ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3750G-24TS-1U</td>
<td>24 10/100/1000 Ethernet ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3750G-48PS</td>
<td>48 10/100/1000 PoE ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3750G-48TS</td>
<td>48 10/100/1000 Ethernet ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3750V2-24PS</td>
<td>24 10/100 PoE ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
<tr>
<td>Catalyst 3750V2-24TS</td>
<td>24 10/100 ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
<tr>
<td>Catalyst 3750V2-48PS</td>
<td>48 10/100 PoE ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
<tr>
<td>Catalyst 3750V2-48TS</td>
<td>48 10/100 ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
<tr>
<td>NME-16ES-1G3</td>
<td>16 10/100 ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide</td>
<td>Cisco IOS Release 12.2(25)SEC</td>
</tr>
<tr>
<td>NME-16ES-1G-P4</td>
<td>16 10/100 PoE ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide</td>
<td>Cisco IOS Release 12.2(25)EZ</td>
</tr>
<tr>
<td>NME-X-23ES-1G3</td>
<td>23 10/100 ports, 1 10/100/1000 PoE port, no StackWise connector ports, single-wide</td>
<td>Cisco IOS Release 12.2(25)SEC</td>
</tr>
<tr>
<td>NME-X-23ES-1G-P4</td>
<td>23 10/100 PoE ports, 1 10/100/1000 PoE port, no StackWise connector ports, extended single-wide</td>
<td>Cisco IOS Release 12.2(25)EZ</td>
</tr>
<tr>
<td>NME-XD-24ES-1S-P4</td>
<td>24 10/100 PoE ports, 1 SFP module port, 2 StackWise connector ports, extended double-wide</td>
<td>Cisco IOS Release 12.2(25)EZ</td>
</tr>
<tr>
<td>NME-XD-48ES-2S-P4</td>
<td>48 10/100 PoE ports, 2 SFP module ports, no StackWise connector ports, extended double-wide</td>
<td>Cisco IOS Release 12.2(25)EZ</td>
</tr>
<tr>
<td>WS-3750V2-24FS</td>
<td>24 SFP module slots and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(55)SE5</td>
</tr>
</tbody>
</table>

1. PoE = Power over Ethernet
2. SFP = small form-factor pluggable
3. Cisco EtherSwitch service module
## Table 2  Catalyst 3560 Switches Supported

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3560-8PC</td>
<td>8 10/100 PoE ports and 1 dual-purpose port(^1) (one 10/100/1000BASE-T copper port and one SFP module slot)</td>
<td>Cisco IOS Release 12.2(35)SE</td>
</tr>
<tr>
<td>Catalyst 3560-24PS</td>
<td>24 10/100 PoE ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3560-24TS</td>
<td>24 10/100 ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3560-48PS</td>
<td>48 10/100 PoE ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Catalyst 3560-48TS</td>
<td>48 10/100 ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3560G-24PS</td>
<td>24 10/100 PoE ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3560G-24TS</td>
<td>24 10/100/1000 Ethernet ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3560G-48PS</td>
<td>48 10/100/1000 PoE ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3560G-48TS</td>
<td>48 10/100/1000 Ethernet ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(20)SE3</td>
</tr>
<tr>
<td>Catalyst 3560-12PC Compact Switch</td>
<td>12 Ethernet 10/100 ports with PoE and 1 dual-purpose 10/100/1000 or SFP uplink</td>
<td>Cisco IOS Release 12.2(50)SE</td>
</tr>
<tr>
<td>Catalyst 3560V2-24PS</td>
<td>24 10/100 PoE ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
<tr>
<td>Catalyst 3560V2-24TS</td>
<td>24 10/100 ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
<tr>
<td>Catalyst 3560V2-48PS</td>
<td>48 10/100 PoE ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
<tr>
<td>Catalyst 3560V2-48TS</td>
<td>48 10/100 ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
<tr>
<td>Catalyst 3560V2-24TS-SD</td>
<td>24 10/100 ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE1</td>
</tr>
</tbody>
</table>

\(^1\) Each uplink port is considered a single interface with dual front ends (RJ-45 connector and SFP module slot). The dual front ends are not redundant interfaces, and only one port of the pair is active.

## Table 3  Catalyst 2975, 2960-S, and 2960 Switches Supported

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 2975GS-48PS-L</td>
<td>48 10/100/1000 PoE ports and 4 SFP module slots</td>
<td>Cisco IOS Release 12.2(46)EX</td>
</tr>
<tr>
<td>Catalyst 2960-48PST-S</td>
<td>48 10/100 PoE ports, 2 10/100/1000 ports, and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(50)SE2</td>
</tr>
<tr>
<td>Catalyst 2960-24PC-S</td>
<td>24 10/100 PoE ports and 2 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(50)SE2</td>
</tr>
<tr>
<td>Catalyst 2960-24LC-S</td>
<td>24 10/100 ports (8 of which are PoE) and 2 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(50)SE2</td>
</tr>
<tr>
<td>Catalyst 2960-8TC-S</td>
<td>8 10/100 ports and 1 dual-purpose port(^1) (1 10/100/1000BASE-T copper port and 1 SFP module slot)</td>
<td>Cisco IOS Release 12.2(46)SE</td>
</tr>
</tbody>
</table>
### Table 3  Catalyst 2975, 2960-S, and 2960 Switches Supported (continued)

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 2960-48TT-S</td>
<td>48 10/100 ports and 1 10/100/1000 ports</td>
<td>Cisco IOS Release 12.2(46)SE</td>
</tr>
<tr>
<td>Catalyst 2960-48PST-L</td>
<td>48 10/100 PoE ports, 1 10/100/1000 ports and 2 SFP module slots</td>
<td>Cisco IOS Release 12.2(46)SE</td>
</tr>
<tr>
<td>Catalyst 2960-24-S</td>
<td>24 10/100 BASE-TX Ethernet ports</td>
<td>Cisco IOS Release 12.2(37)EY</td>
</tr>
<tr>
<td>Catalyst 2960-24TC-S</td>
<td>24 10/100BASE-T Ethernet ports and 2 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(37)EY</td>
</tr>
<tr>
<td>Catalyst 2960-48TC-S</td>
<td>48 10/100BASE-T Ethernet ports and 2 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(37)EY</td>
</tr>
<tr>
<td>Catalyst 2960PD-8TT-L</td>
<td>8 10/100 ports and 1 10/100/1000 port that receives power</td>
<td>Cisco IOS Release 12.2(44)SE</td>
</tr>
<tr>
<td>Catalyst 2960-8TC-L</td>
<td>8 10/100 Ethernet ports and 1 dual-purpose port</td>
<td>Cisco IOS Release 12.2(35)SE</td>
</tr>
<tr>
<td>Catalyst 2960G-8TC-L</td>
<td>7 10/100/1000 Ethernet ports and 1 dual-purpose port</td>
<td>Cisco IOS Release 12.2(35)SE</td>
</tr>
<tr>
<td>Catalyst 2960-24LT-L</td>
<td>24 10/100 ports, 8 of which are PoE, and 2 10/100/1000 ports</td>
<td>Cisco IOS Release 12.2(44)SE</td>
</tr>
<tr>
<td>Catalyst 2960-48TC-L</td>
<td>48 10/100BASE-TX Ethernet ports and 2 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(25)FX</td>
</tr>
<tr>
<td>Catalyst 2960-24TC-L</td>
<td>24 10/100BASE-TX Ethernet ports and 2 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(25)FX</td>
</tr>
<tr>
<td>Catalyst 2960-24PC-L</td>
<td>24 10/100 Power over Ethernet (PoE) ports and 2 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(44)SE</td>
</tr>
<tr>
<td>Catalyst 2960-24TT-L</td>
<td>24 10/100BASE-T Ethernet ports and 2 10/100/1000BASE-T Ethernet ports</td>
<td>Cisco IOS Release 12.2(25)FX</td>
</tr>
<tr>
<td>Catalyst 2960-48TT-L</td>
<td>48 10/100BASE-T Ethernet ports 2 10/100/1000BASE-T Ethernet ports</td>
<td>Cisco IOS Release 12.2(25)FX</td>
</tr>
<tr>
<td>Catalyst 2960G-24TC-L</td>
<td>24 10/100/1000BASE-T Ethernet ports, including 4 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(25)FX</td>
</tr>
<tr>
<td>Catalyst 2960G-48TC-L</td>
<td>48 10/100/1000BASE-T Ethernet ports, including 4 dual-purpose ports</td>
<td>Cisco IOS Release 12.2(25)SEE</td>
</tr>
</tbody>
</table>
System Requirements

Table 4  Other Supported Hardware

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP modules (Catalyst 2960)</td>
<td>1000BASE-BX, -CWDM, -LX/LH, -SX, -ZX, 100BASE-BX, FX, -LX</td>
<td>Cisco IOS Release 12.2(25)FX</td>
</tr>
<tr>
<td>XENPAK modules(^3)</td>
<td>XENPAK-10-GB-ER, XENPAK-10-GB-LR, and XENPAK-10-GB-SR</td>
<td>Cisco IOS Release 12.2(18)SE</td>
</tr>
<tr>
<td>Redundant power systems</td>
<td>Cisco RPS 675 Redundant Power System Cisco RPS 300 Redundant Power System (supported only on the Catalyst 2960 switch) Cisco Redundant Power System 2300</td>
<td>Supported on all software releases Supported on all software releases Cisco IOS Release 12.2(35)SE and later</td>
</tr>
</tbody>
</table>

1. CWDM = coarse wavelength-division multiplexer
2. MMF = multimode fiber
3. XENPAK modules are only supported on the Catalyst 3750G-16TD switches.

Device Manager System Requirements

- **Hardware Requirements**, page 6
- **Software Requirements**, page 6

Hardware Requirements

| Table 5  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

- Internet Explorer 6.0 or 7.0, and Firefox up to version 27, with JavaScript enabled.

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

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

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

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3750 switch, all standby command switches must be Catalyst 3750 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/pcgi-bin/tablebuild.pl/NetworkAssistant

For more information about Cisco Network Assistant, see the [Release Notes for Cisco Network Assistant](#) on Cisco.com.

Upgrading the Switch Software

- Finding the Software Version and Feature Set, page 7
- Deciding Which Files to Use, page 8
- Catalyst 3750G Integrated Wireless LAN Controller Switch Software Compatibility, page 9
- Archiving Software Images, page 9
- Upgrading a Switch by Using the Device Manager or Network Assistant, page 10
- Upgrading a Switch by Using the CLI, page 10
- Recovering from a Software Failure, page 11

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**

For Catalyst 3750 and 3560 switches and the Cisco EtherSwitch service modules, 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 (IP base image or IP services image) and does not change if you upgrade the software image.

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 6  Cisco IOS Software Image Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3750-ipbasek9-tar.122-55.SE1.tar</td>
<td>Catalyst 3750 IP base cryptographic image and device manager files. This image has the Kerberos, SSH¹, Layer 2+, and basic Layer 3 routing features. This image also runs on the Cisco EtherSwitch service modules.</td>
</tr>
<tr>
<td>c3750-ipbaselmk9-tar.122-55.SE1.tar</td>
<td>Catalyst 3750 IP base cryptographic image with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.</td>
</tr>
<tr>
<td>c3750-ipservicesk9-tar.122-55.SE1.tar</td>
<td>Catalyst 3750 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features. This image also runs on the Cisco EtherSwitch service modules.</td>
</tr>
<tr>
<td>c3750-ipserviceslmk9-tar.122-55.SE1.tar</td>
<td>Catalyst 3750 IP services cryptographic image with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.</td>
</tr>
<tr>
<td>c3560-ipbasek9-tar.122-55.SE1.tar</td>
<td>Catalyst 3560 IP base cryptographic image and device manager files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.</td>
</tr>
<tr>
<td>c3560-ipbaselmk9-tar.122-55.SE1.tar</td>
<td>Catalyst 3560 IP base cryptographic image with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.</td>
</tr>
<tr>
<td>c3560-ipservicesk9-tar.122-55.SE1.tar</td>
<td>Catalyst 3560 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.</td>
</tr>
<tr>
<td>c3560-ipserviceslmk9-tar.122-55.SE1.tar</td>
<td>Catalyst 3560 IP services cryptographic image with device manager Express Setup files only. This image is intended for switches that have a 16M flash size.</td>
</tr>
<tr>
<td>c2975-lanbasek9-tar.122-55.SE.tar</td>
<td>Catalyst 2975 cryptographic image file and device manager files. This image has the Kerberos and SSH features.</td>
</tr>
<tr>
<td>c2960-lanbasek9-tar.122-55.SE.tar</td>
<td>Catalyst 2960 cryptographic image file and device manager files. This image has the Kerberos and SSH features.</td>
</tr>
<tr>
<td>c2960-lanlitek9-tar.122-55.SE.tar</td>
<td>Catalyst 2960 LAN lite cryptographic image file and device manager files.</td>
</tr>
<tr>
<td>c2960s-universalk9-tar.122-55.SE2.tar</td>
<td>LAN Base and LAN Lite crypto image with device manager</td>
</tr>
</tbody>
</table>

¹ SSH = Secure Shell.
Catalyst 3750G Integrated Wireless LAN Controller Switch Software Compatibility

The Catalyst 3750 Integrated Wireless LAN Controller Switch is an integrated Catalyst 3750 switch and Cisco 4400 series wireless LAN controller that supports up to 25 or 50 lightweight access points. The switch and the internal controller run separate software versions, which must be upgraded separately.

To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running one of these Cisco IOS software releases:

- Cisco IOS Release 12.2(25)FZ
- Cisco IOS Release 12.2(35)SE or later
- Cisco IOS Release 12.2(37)SE or later
- Cisco IOS Release 12.2(44)SE or later
- Cisco IOS Release 12.2(46)SE or later

Note These Cisco IOS Releases and any versions of them are not supported: Cisco IOS Release 12.2(25)SEC, 12.2(25)SED, 12.2(25)SEE, 12.2(25)SEF, and 12.2(25)SEG. All Catalyst 3750 images (IP Base, IP Services, and Advanced IP Services) are supported for use with the controller.

If the switch image version is not compatible, the wireless LAN controller switch could stop functioning.

For information about the controller software, see the release notes on this page for Cisco Software Release 4.0.x.0 or later:

For controller software upgrade procedure, see the Cisco Wireless LAN Controller Configuration Guide on this page:

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:

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

Note Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.
You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the `tftp-server` global configuration command. For more information about the `tftp-server` command, see the “Basic File Transfer Services Commands” section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*: http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

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

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

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

**Upgrading a Switch by Using the CLI**

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

To download software, follow these steps:

**Step 1** Use Table 6 on page 8 to identify the file that you want to download.

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

a. If you are a registered customer, go to this URL and log in.


c. Navigate to your switch model.

d. Click IOS Software, then select the latest IOS release.

Download the image you identified in Step 1.

**Caution** If you are upgrading a Catalyst 3750 switch that is running a release earlier than Cisco IOS Release 12.1(19)EA1c, this release includes a bootloader upgrade. The bootloader can take up to 1 minute to upgrade the first time that the new software is loaded. Do not power cycle the switch during the bootloader upgrade.

**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.

---

**Note**

If you are upgrading a Catalyst 3750 or a 2950 switch running Cisco IOS Release 12.1(11)AX, which uses the IEEE 802.1x feature, you must re-enable IEEE 802.1x after upgrading the software. For more information, see the “Cisco IOS Notes” section on page 36.
**New Software Features**

- Support for critical voice VLAN to so that when authentication is enabled and the access control server is not available, traffic from the host tagged with the voice VLAN is put into the configured voice VLAN for the port. (Applicable for Cisco IOS Release 12.2(55)SE5 and higher)
  
  See the “Documentation Updates” section on page 66.
- Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices, such as the Cisco Telepresence System and Cisco Surveillance Camera.
- AutoSmartport enhancements, which add support for global macros, last-resort macros, event trigger control, access points, EtherChannels, auto-QoS with Cisco Medianet, and IP phones.
- Support for CDP and LLDP enhancements for exchanging location information with video end points for dynamic location-based content distribution from servers.
- Smart Install enhancements supporting client backup files, zero-touch replacement for clients with the same product-ID, automatic generation of the imagelist file, configurable file repository, hostname changes, transparent connection of the director to client, USB storage for image and seed configuration, and changes in `show` command outputs.
- Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs configured.
- Support for VLAN assignment on a port configured for multi-auth mode. The RADIUS server assigns a VLAN to the first host to authenticate on the port, and subsequent hosts use the same VLAN. Voice VLAN assignment is supported for one IP phone.
- Memory consistency check routines to detect and correct invalid ternary content addressable memory (TCAM) table entries. (Not supported on Catalyst 2960-S)
- When you configure the new `lanbase-routing` SDM template, the switch supports static routing and router ACLs on SVIs. (Catalyst 2960, 2960-S, and 2975)
- Support for the Security Group Tag (SCT) Exchange Protocol (SXP) component of Cisco TrustSec, a security architecture using authentication, encryption, and access control (Catalyst 3750 and 3560)
- AAA guarantee-first support for enabling or disabling system accounting as the first record.
- An option to suppress verbose 802.1x, authentication manager, and MAC authentication bypass syslog messages.
- Support for Embedded Event Manager (EEM) in the IP base image. (Catalyst 3750 and 3560)
- Support for QoS class-default policy placement.
- Improvements in QoS policing granularity by changing the range for the rate-bps value from 1000000 through 1000000000 to 8000 through 1000000000. (Catalyst 2960 and 2975)
- Support for LLDP-MED and DHCP snooping with Option 82 on the LAN Lite image. (Catalyst 2960-S, 2960, and 2975)
• The IP Base image supports OSPF for routed access to enable customers to extend Layer 3 routing capabilities to the access or wiring closet. The IP services image is required if you need multiple OSPFv2 and OSPFv3 instances without route restrictions. (Catalyst 3750 and 3560)
• MAC move to allow hosts (including the hosts connected to an IP 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 as a completely new MAC address. MAC replace can be configured so that when a host disconnects from a port without ending its session, the session can be ended and the authentication sequence reset when a new MAC address connects to the port.
• Support for increasing the NVRAM buffer size for saving large configuration files.
• ARP tracking probe enhancement to specify a source IP address for a VLAN.
• Network Edge Access Topology (NEAT) controls the supplicant port during the supplicant authentication period. When you connect a supplicant switch to the authenticator switch, the authenticator port could be error-disabled when receiving Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets and the supplicant switch is not authenticated. The NEAT feature is now enhanced to block the supplicant port during authentication, to ensure authentication completes.

Use the `dot1x supplicant controlled transient` global configuration command to control access to the supplicant port during authentication. Use the `no` form of this command to provide access to the supplicant port during the authentication period.
• CISCO-ENERGYWISE-MIB enhancements. See the Release Notes for Cisco EnergyWise, EnergyWise Phase 2 for information. (Catalyst 3750, 3560, 2960-S, and 2960)

**Minimum Cisco IOS Release for Major Features**

Table 7 lists the minimum software release required to support the major features of the Catalyst 3750, 3560, 2975, 2960-S and 2960 switches and the Cisco EtherSwitch service modules.

---

**Table 7**  
*Catalyst 3750 and 3560, 2975, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum Cisco IOS Release Required</th>
<th>Catalyst Switch Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-QoS enhancements</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2975, 2960-S</td>
</tr>
<tr>
<td>Auto Smartport enhancements including global macros</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2975, 2960-S</td>
</tr>
<tr>
<td>Smart Install enhancements and new features</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2975, 2960-S</td>
</tr>
<tr>
<td>Port ACL improvements</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2975, 2960-S</td>
</tr>
<tr>
<td>CDP and LLDP location enhancements</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2975, 2960-S</td>
</tr>
<tr>
<td>Multi-authentication with VLAN assignment</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2975, 2960-S</td>
</tr>
<tr>
<td>Cisco TrustSec</td>
<td>12.2(55)SE</td>
<td>3750 and 3560</td>
</tr>
<tr>
<td>Memory-consistency check routines</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>Static routing support on SVIs</td>
<td>12.2(55)SE</td>
<td>2975, 2960, and 2960-S</td>
</tr>
<tr>
<td>MAC replace to end a session when a host disconnects from a port</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2975, 2960-S</td>
</tr>
</tbody>
</table>

---

Release Notes for the Catalyst 3750, 3560, 2975, 2960-S, and 2960 Switches, Cisco IOS Release 12.2(55)SE and Later

OL-23054-07
## Table 7  Catalyst 3750 and 3560, 2975, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum Cisco IOS Release Required</th>
<th>Catalyst Switch Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP snooping and Option 82 and LLDP-MED in LAN lite image</td>
<td>12.2(55)SE</td>
<td>2960 and 2960-S</td>
</tr>
<tr>
<td>Smart Install to allow a single point of management (director) in a network.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>Support for IP source guard on static hosts.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>AutoSmartPort enhancements (macro persistency, LLDP-based triggers, MAC address and OUI-based triggers, remote macros).</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>RADIUS Change of Authorization (CoA).</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>802.1x User Distribution for deployments with multiple VLANs.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>Critical VLAN with multiple-host authentication.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>Customizable web authentication enhancement to allow the creation of user-defined pages.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>Network Edge Access Topology (NEAT) to change the port host mode.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>VLAN-ID based MAC authentication.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>MAC move to allow hosts to move across ports on the same switch.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>3DES and AES with SNMPv3.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>Hostname support in the option 12 field of DHCPDISCOVER packets.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>DHCP Snooping enhancement for the circuit-id sub-option.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>Increased support for LLDP-MED</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>LLDP-MED MIB and the CISCO-ADMISSION-POLICY-MIB.</td>
<td>12.2(52)SE</td>
<td>3750, 3560, 2975, 2960</td>
</tr>
<tr>
<td>IPv6 QoS trust capability.</td>
<td>12.2(52)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Cisco Medianet to enable intelligent services in the network infrastructure for video applications.</td>
<td>12.2(52)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>EEM 3.2 event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.</td>
<td>12.2(52)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Cisco EnergyWise Phase 2 to manage EnergyWise-enabled Cisco devices and non-Cisco end points running EnergyWise agents.</td>
<td>12.2(55)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>802.1x with open access</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>802.1x authentication with downloadable ACLs and redirect URLs</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Flexible-authentication sequencing</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Multiple-user authentication</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Cisco EnergyWise Phase 1 to manage power usage over PoE devices.</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Wired location service</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
</tbody>
</table>
## Table 7  Catalyst 3750 and 3560, 2975, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum Cisco IOS Release Required</th>
<th>Catalyst Switch Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU utilization threshold trap</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Cisco IOS Configuration Engine (previously the Cisco IOS CNS agent)</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>LLDP-MED network-policy profile time, length, value (TLV)</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>RADIUS server load balancing</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Auto Smartports Cisco-default and user-defined macros</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>SCP attribute support in the CONFIG_COPY MIB, CISCO-AUTH-FRAMEWORK-MIB, CISCO-MAC-AUTH-BYPASS MIBs, LLDP MIB</td>
<td>12.2(50)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Intermediate System-to-Intermediate System (IS-IS) routing for Connectionless Network Service (CLNS) networks</td>
<td>12.2(50)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Support for Embedded Event Manager Version 2.4.</td>
<td>12.2(50)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>IPv6 features in the IP services and IP base images: ACLs; DHCPv6 for the DCHP server, client, and relay device; EIGRPv6; HSRPv6; OSPFv3; RIP; Static routes</td>
<td>12.2(50)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Stack troubleshooting enhancements</td>
<td>12.2(50)SE</td>
<td>3750</td>
</tr>
<tr>
<td>802.1x authentication with restricted VLANs</td>
<td>12.2(50)SE</td>
<td>2960</td>
</tr>
<tr>
<td>IP source guard</td>
<td>12.2(50)SE</td>
<td>2960</td>
</tr>
<tr>
<td>Dynamic ARP inspection</td>
<td>12.2(50)SE</td>
<td>2960</td>
</tr>
<tr>
<td>Generic message authentication support with SSH Protocol and compliance with RFC 4256</td>
<td>12.2(46)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Generic message authentication support</td>
<td>12.2(46)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Disabling MAC address learning on a VLAN</td>
<td>12.2(46)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>PAgP Interaction with Virtual Switches and Dual-Active Detection</td>
<td>12.2(46)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>DHCP server port-based address allocation</td>
<td>12.2(46)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>IPv6 default router preference (DRP)</td>
<td>12.2(46)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Voice aware IEEE 802.1x and mac authentication bypass (MAB) security violation</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Local web authentication banner</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Support for the CISCO-NAC-NAD and CISCO-PAE MIBs</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Excluding a port in a VLAN from the SVI line-state calculation</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>EOT and IP SLAs EOT static route support</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Support for HSRP Version 2 (HSRPv2)</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>HSRP for IPv6 (advanced IP services image)</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>DHCP for IPv6 relay, client, server address assignment and prefix delegation (advanced IP services image)</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
</tbody>
</table>
### Table 7  
**Catalyst 3750 and 3560, 2975, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum Cisco IOS Release Required</th>
<th>Catalyst Switch Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded event manager (EEM) (IP services image only)</td>
<td>12.2(46)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)</td>
<td>12.2(46)SE</td>
<td>2960</td>
</tr>
<tr>
<td>Monitoring real-time power consumption on a per-PoE port basis</td>
<td>12.2(46)SE</td>
<td>2960</td>
</tr>
<tr>
<td>IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute</td>
<td>12.2(46)SE</td>
<td>2960</td>
</tr>
<tr>
<td>IEEE 802.1x readiness check</td>
<td>12.2(44)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>DHCP-based autoconfiguration and image update</td>
<td>12.2(44)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Configurable small-frame arrival threshold</td>
<td>12.2(44)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>HTTP and HTTP(s) support over IPv6</td>
<td>12.2(44)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>SNMP configuration over IPv6 transport</td>
<td>12.2(44)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>IPv6 stateless autoconfiguration</td>
<td>12.2(44)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Flex Link Multicast Fast Convergence</td>
<td>12.2(44)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Digital optical monitoring (DOM)</td>
<td>12.2(44)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Source Specific Multicast (SSM) mapping</td>
<td>12.2(44)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>/31 bit mask support for multicast traffic</td>
<td>12.2(44)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Configuration replacement and rollback</td>
<td>12.2(40)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol Media Extensions (LLDP-MED)</td>
<td>12.2(40)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6</td>
<td>12.2(40)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Automatic quality of service (QoS) Voice over IP (VoIP)</td>
<td>12.2(40)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Dynamic voice virtual LAN (VLAN) for MDA-enabled ports</td>
<td>12.2(40)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Internet Group Management Protocol (IGMP) helper</td>
<td>12.2(40)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>IP Service Level Agreements (IP SLAs)</td>
<td>12.2(40)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>IP SLAs EOT</td>
<td>12.2(40)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Multicast virtual routing and forwarding (VRF) lite</td>
<td>12.2(40)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>SSM PIM protocol</td>
<td>12.2(40)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>VRF-aware support for HSRP, uRPF, ARP, SNMP, IP SLA, TFTP, FTP, syslog, traceroute, and ping</td>
<td>12.2(40)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>MLD snooping</td>
<td>12.2(40)SE</td>
<td>2960</td>
</tr>
<tr>
<td>IPv6 host</td>
<td>12.2(40)SE</td>
<td>2960</td>
</tr>
<tr>
<td>IP phone detection enhancement</td>
<td>12.2(37)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED)</td>
<td>12.2(37)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>PIM stub routing</td>
<td>12.2(37)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Port security on a PVLAN host</td>
<td>12.2(37)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Feature</td>
<td>Minimum Cisco IOS Release Required</td>
<td>Catalyst Switch Support</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>VLAN aware port security option</td>
<td>12.2(37)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Auto rendezvous point (auto-RP) for multicast</td>
<td>12.2(37)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>VLAN Flex Links load balancing</td>
<td>12.2(37)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Web Cache Communication Protocol (WCCP)</td>
<td>12.2(37)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Multidomain authentication (MDA)</td>
<td>12.2(35)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Web authentication</td>
<td>12.2(35)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>MAC inactivity aging</td>
<td>12.2(35)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Support for IPv6 with Express Setup</td>
<td>12.2(35)SE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Generic online diagnostics</td>
<td>12.2(35)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Stack MAC persistent timer and archive download enhancements</td>
<td>12.2(35)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>HSRP enhanced object tracking</td>
<td>12.2(35)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>OSPF and EIGRP Nonstop forwarding capability (IP services image only)</td>
<td>12.2(35)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>IPv6 router ACLs for inbound Layer 3 management traffic</td>
<td>12.2(35)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Generic online diagnostics to test the hardware functionality of the supervisor engine</td>
<td>12.2(25)SEE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>DHCP Option 82 configurable remote ID and circuit ID</td>
<td>12.2(25)SEE</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>EIGRP stub routing in the IP base image</td>
<td>12.2(25)SEE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>/31 bit mask support for unicast traffic</td>
<td>12.2(25)SEE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Access SDM templates</td>
<td>12.2(25)SED</td>
<td>3750, 3560 Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>IPv6 ACLs</td>
<td>12.2(25)SED</td>
<td>3750, 3560 Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>IPv6 Multicast Listener Discovery (MLD) snooping</td>
<td>12.2(25)SED</td>
<td>3750, 3560 Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>QoS hierarchical policy maps on a port</td>
<td>12.2(25)SED</td>
<td>3750, 3560 Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>NAC Layer 2 IEEE 802.1x validation</td>
<td>12.2(25)SED</td>
<td>3750, 3560, 2960 Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>NAC Layer 2 IP validation</td>
<td>12.2(25)SED</td>
<td>3750, 3560 Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>IEEE 802.1x inaccessible authentication bypass.</td>
<td>12.2(25)SED</td>
<td>3750, 3560 Cisco EtherSwitch service module 2960</td>
</tr>
<tr>
<td>IEEE 802.1x with restricted VLAN</td>
<td>12.2(25)SED</td>
<td>3750, 3560 Cisco EtherSwitch service modules</td>
</tr>
</tbody>
</table>
### Table 7  
**Catalyst 3750 and 3560, 2975, 2960-S and 2960 Switches and Cisco EtherSwitch Service Module Features and the Minimum Cisco IOS Release Required (continued)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum Cisco IOS Release Required</th>
<th>Catalyst Switch Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budgeting power for devices connected to PoE ports</td>
<td>12.2(25)SEC, 12.2(25)SED</td>
<td>3750, 3560, Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>Multiple spanning-tree (MST) based on the IEEE 802.1s standard</td>
<td>12.2(25)SEC, 12.2(25)SED</td>
<td>3750, 3560, Cisco EtherSwitch service modules, 2960</td>
</tr>
<tr>
<td>Unique device identifier (UDI)</td>
<td>12.2(25)SEC, 12.2(25)SED</td>
<td>3750, 3560, Cisco EtherSwitch service modules, 2960</td>
</tr>
<tr>
<td>VRF Lite</td>
<td>12.2(25)SEC</td>
<td>3750, 3560, Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>IEEE 802.1x with wake-on-LAN</td>
<td>12.2(25)SEC, 12.2(25)SED</td>
<td>3750, 3560, 2960, Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>Nonstop forwarding (NSF) awareness</td>
<td>12.2(25)SEC</td>
<td>3750, 3560, Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>Configuration logging</td>
<td>12.2(25)SEC, 12.2(25)SED</td>
<td>3750, 3560, 2960, Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>Secure Copy Protocol</td>
<td>12.2(25)SEC, 12.2(25)SED</td>
<td>3750, 3560, 2960, Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>Cross-stack EtherChannel</td>
<td>12.2(25)SEC</td>
<td>3750, Cisco EtherSwitch service modules</td>
</tr>
<tr>
<td>Private-VLAN on interfaces configured for dynamic ARP inspection</td>
<td>12.2(25)SEB</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>IP source guard on private VLANs</td>
<td>12.2(25)SEB</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>IEEE 802.1x restricted VLAN</td>
<td>12.2(25)SED</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>IGMP leave timer</td>
<td>12.2(25)SEB, 12.2(25)SED</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>IGMP snooping querier</td>
<td>12.2(25)SEA, 12.2(25)FX</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>Advanced IP services</td>
<td>12.2(25)SEA, 12.2(25)FX</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>DSCP transparency</td>
<td>12.2(25)SE, 12.2(25)FX</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>VLAN-based QoS&lt;sup&gt;1&lt;/sup&gt; and hierarchical policy maps on SVIs&lt;sup&gt;2&lt;/sup&gt;</td>
<td>12.2(25)SE</td>
<td>3750, 3560</td>
</tr>
<tr>
<td>Device manager</td>
<td>12.2(25)SE, 12.2(25)FX</td>
<td>3750, 3560, 2960</td>
</tr>
<tr>
<td>IEEE 802.1Q tunneling and Layer 2 protocol tunneling</td>
<td>12.2(25)SE</td>
<td>3750, 3560</td>
</tr>
</tbody>
</table>
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 20
- **Device Manager Limitations**, page 35
Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 3750 and 3560, and 2960 switches and the Cisco EtherSwitch service modules:

- Configuration, page 20
- Ethernet, page 23
- EtherSwitch Modules, page 24
- Fallback Bridging, page 24
- HSRP, page 24
- IP, page 25
- IP Telephony, page 25
- MAC Addressing, page 25
- MAC Addressing, page 25
- Multicasting, page 26
- Power, page 27
- QoS, page 28
- Routing, page 28
- Smart Install, page 29
- SPAN and RSPAN, page 30
- Stacking (Catalyst 3750 or Cisco EtherSwitch service module switch stack only), page 32
- Trunking, page 34
- VLAN, page 35

Configuration

- A static IP address might be removed when the previously acquired DHCP IP address lease expires. This problem occurs under these conditions:
  - When the switch is booted up without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.
  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)
- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When the show interface privileged EXEC is entered on a port that is running IEEE 802.1Q, inconsistent statistics from ports running IEEE 802.1Q might be reported. The workaround is to upgrade to Cisco IOS Release 12.1(20)EA1. (CSCec35100)
Limitations and Restrictions

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When you change a port from a nonrouted port to a routed port or the reverse, the applied auto-QoS setting is not changed or updated when you verify it by using the `show running interface` or `show mls qos interface` user EXEC commands. These are the workarounds:
  1. Disable auto-QoS on the interface.
  2. Change the routed port to a nonrouted port or the reverse.
  3. Re-enable auto-QoS on the interface. (CSCec44169)

- 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)

- The DHCP snooping binding database is not written to flash memory or a remote file in any of these situations:
  - (Catalyst 3750 switch and Cisco EtherSwitch service modules) When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the `show NTP status` privileged EXEC command and verifying that the network connection to the NTP server and the peer work correctly.
  - (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. If the file is manually removed from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
  - (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The URL for the configured DHCP snooping database was replaced because the original URL was not accessible. The new URL might not take effect after the timeout of the old URL. No workaround is necessary; these are the designed behaviors. (CSCed50819)

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails are lost. When you enter the `show ip arp inspection log` privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which you entered the command. There is no workaround. (CSCed95822)

- 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)

- (Cisco EtherSwitch service modules) You cannot change the console baud rate by using the switch CLI. The console on the Cisco EtherSwitch service modules only supports three baud rates (9600 b/s, 19200 b/s, and 38400 b/s) and must be set at the bootloader prompt. The switch rejects a CLI command to change the baud rate.
  To change the baud rate, reload the Cisco EtherSwitch service module with the bootloader prompt. You can then change the baud rate and change the speed on the TTY line of the router connected to the Cisco EtherSwitch Service module console.
  There is no workaround. (CSCeh50152)

- When a Catalyst 3750-12S switch boots up, ports 2, 6, and 10 can become active before the Cisco IOS software loading process is complete. Packets arriving at these ports before the switch software is completely loaded are lost. This is a hardware limitation when the switch uses small form-factor pluggable (SFP) modules with copper connections.
  The workaround is to use switch ports other than those specified for redundancy and for applications that immediately detect active links. (CSCeh70503)

- 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:

  ```text
  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
  (CSCsh12472 [Catalyst 3750 and 3560 switches])
  ```

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.
  The workaround is to configure aggressive UDLD. (CSCsh70244).

- 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 the configuration file is removed from the switch and the switch is rebooted, port status for VLAN 1 and the management port (Fast Ethernet 0) is sometimes reported as `up` and sometimes as `down`, resulting in conflicts. This status depends on when you respond to the reboot query:

  Would you like to enter the initial configuration dialog?
  - After a reboot if you wait until the Line Protocol status of VLAN 1 appears on the console before responding, VLAN 1 line status is always shown as `down`. This is the correct state.
  - The problem (VLAN 1 reporting `up`) occurs if you respond to the query before VLAN 1 line status appears on the console.

  The workaround is to wait for approximately 1 minute after rebooting and until the VLAN 1 interface line status appears on the console before you respond to the query. (CSCsl02680) (Catalyst 3750 and 3560 switches)
• A T-start error message appears after startup under these conditions:
  – Two-link ports on the same switch are connected with a crossover cable.
  – The switch is running Cisco IOS 12.2(50)SE3 or later.

The workaround is to connect the two ports with a straight-through cable. (CSCsr41271)
(Catalyst 3750V2 and Catalyst 3560V2 PoE switches and Cisco Etherswitch service modules only)

• 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)

• 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**

• Link connectivity might be lost between some older models of the Intel Pro1000 NIC and the 10/100/1000 switch port interfaces. The loss of connectivity occurs between the NIC and these switch ports:
  – Ports 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 23, and 24 of the Catalyst 3750G-24T and 3750G-24TS switches
  – Gigabit Ethernet ports on the Cisco EtherSwitch service modules

These are the workarounds:
  – Contact the NIC vendor, and get the latest driver for the card.
  – Configure the interface for 1000 Mb/s instead of for 10/100 Mb/s.
  – Connect the NIC to an interface that is not listed here. (CSCea77032)

For more information, enter CSCea77032 in the Bug Toolkit at this URL:
http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl

• (Cisco EtherSwitch service modules) When a Cisco EtherSwitch service module reloads or the internal link resets, there can be up to a 45-second delay in providing power to PoE devices, depending on the configuration. If the internal Gigabit Ethernet interface on a Cisco EtherSwitch service module connected to the router is configured as a switch port in access mode or in trunk mode, the internal link is not operational until it reaches the STP forwarding state. Therefore, the PoE that comes from the host router is also not available until the internal Gigabit Ethernet link reaches the STP forwarding state. This is due to STP convergence time. This problem does not occur on routed ports.

If the Cisco EtherSwitch service module is in access mode, the workaround is to enter the spanning-tree portfast interface configuration command on the internal Gigabit Ethernet interface. If the service module is in trunk mode, there is no workaround.

• 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)

**EtherSwitch Modules**

- A duplex mismatch occurs when two Fast Ethernet interfaces that are directly connected on two EtherSwitch service modules are configured as both 100 Mb/s and full duplex and as automatic speed and duplex settings. This is expected behavior for the PHY on the Cisco EtherSwitch service modules.

  There is no workaround. (CSCeh35595)

**Fallback Bridging**

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) If a bridge group contains a VLAN to which a static MAC address is configured, all non-IP traffic in the bridge group with this MAC address destination is sent to all ports in the bridge group. The workaround is to remove the VLAN from the bridge group or to remove the static MAC address from the VLAN. (CSCdw81955)

  - (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) Known unicast (secured) addresses are flooded within a bridge group if secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group. Non-IP traffic destined to the secure addresses is flooded within the bridge group. The workaround is to disable fallback bridging or to disable port security on all ports in all VLANs participating in fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the `no bridge-group bridge-group` interface configuration command. To disable port security on all ports in all VLANs participating in fallback bridging, use the `no switchport port-security` interface configuration command. (CSCdz80499)

**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)
Limitations and Restrictions

IP

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out. The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)

- 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)

- (Catalyst 3750 or 3560 PoE-capable switches and Cisco EtherSwitch service modules) The switch uses the IEEE classification to learn the maximum power consumption of a powered device before powering it. The switch grants power only when the maximum wattage configured on the port is less than or equal to the IEEE class maximum. This ensures that the switch power budget is not oversubscribed. There is no such mechanism in Cisco prestandard powered devices.

The workaround for networks with pre-standard powered devices is to leave the maximum wattage set at the default value (15.4 W). You can also configure the maximum wattage for the port for no less than the value the powered device reports as the power consumption through CDP messages. For networks with IEEE Class 0, 3, or 4 devices, do not configure the maximum wattage for the port at less than the default 15.4 W (15,400 milliwatts). (CSCee80668)

- Phone detection events that are generated by many IEEE phones connected to the switch ports can consume a significant amount of CPU time if the switch ports cannot power the phones because the internal link is down.

The workaround is to enter the power inline never interface configuration command on all the Fast Ethernet ports that are not powered by but are connected to IP phones if the problem persists. (CSCef84975, Cisco EtherSwitch service modules only)

- 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)

MAC Addressing

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped. (CSCeb67937)

Management

CiscoWorks is not supported on the Catalyst 3750-24FS switch.
Multicasting

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) Nonreverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem occurs for the non-RPF traffic. (CSCdu25219)

- 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)

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) When you use the ip access-group interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)

- (Catalyst 3750 switch stack) If the stack master is power cycled immediately after you enter the ip mroute global configuration command, there is a slight chance that this configuration change might be lost after the stack master changes. This occurs because the stack master did not have time to propagate the running configuration to all the stack members before it was powered down. This problem might also affect other configuration commands. There is no workaround. (CSCea71255)

- (Catalyst 3750 switches and Cisco EtherSwitch service modules) When you enable IP Protocol-Independent Multicast (PIM) on a tunnel interface, the switch incorrectly displays the Multicast is not supported on tunnel interfaces error message. IP PIM is not supported on tunnel interfaces. There is no workaround. (CSCeb75366)

- 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)

- If IP routing is disabled and IP multicast routing is enabled on a switch running Cisco IOS Release 12.2(25)SED, IGMP snooping floods multicast packets to all ports in a VLAN.

The workaround is to enable IP routing or to disable multicast routing on the switch. You can also use the `ip igmp snooping querier` global configuration command if IP multicast routing is enabled for queries on a multicast router port. (CSCsc02995)

### Power

- Non-PoE devices attached to a network might be erroneously detected as an IEEE 802.3af-compliant powered device and powered by the Cisco EtherSwitch service module.

  There is no workaround. You should use the `power inline never` interface configuration command on Cisco EtherSwitch service module ports that are not connected to PoE devices. (CSCee71979)

- When you enter the `show power inline` privileged EXEC command, the output shows the total power used by all Cisco EtherSwitch service modules in the router. The remaining power shown is available for allocation to switching ports on all Cisco EtherSwitch service modules in the router.

  To display the total power used by a specific EtherSwitch service module, enter the `show power inline` command on the router. This output appears:

  ```
  Router# show power inline
  PowerSupply SlotNum. Maximum Allocated Status
  INT-PS 0 360.000 121.000 PS1 GOOD PS2 ABSENT
  Interface Config Device Powered PowerAllocated
  Gi4/0 auto Unknown On 121.000 Watts
  ```

  This is not a problem because the display correctly shows the total used power and the remaining power available on the system. (CSCeg74337)
- 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:

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

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

### RADIUS

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

  There is no workaround. (CSCta05071)

### Routing

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported. There is no workaround. (CSCea52915)

- On a Catalyst 3750 or a Cisco EtherSwitch service module switch stack with a large number of switched virtual interfaces (SVIs), routes, or both on a fully populated nine-member switch stack, this message might appear when you reload the switch stack or add a switch to the stack:

  ```plaintext
  %SYS-2-MALLOCFAIL: Memory allocation of 4252 bytes failed from 0x179C80, alignment 0
  Pool: I/O Free: 77124 Cause: Memory fragmentation
  Alternate Pool: None Free: 0 Cause: No Alternate pool
  ```

  This error message means there is a temporary memory shortage that normally recovers by itself. You can verify that the switch stack has recovered by entering the `show cef line user EXEC` command and verifying that the line card states are `up` and `sync`. No workaround is required because the problem is self-correcting. (CSCea71611)
Limitations and Restrictions

(Catalyst 3750 switches and Cisco EtherSwitch service modules) A spanning-tree loop might occur if all of these conditions are true:

- Port security is enabled with the violation mode set to protected.
- The maximum number of secure addresses is less than the number of switches connected to the port.
- There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

The workaround is to change any one of the listed conditions. (CSCed53633)

Smart Install

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

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

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

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

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

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

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

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

- When the backup configuration is stored in a remote repository, enter the location of the repository.
- When the backup file is stored in the director flash memory, you must manually set the permissions for the file before you enter the `vstack download config` command. (CSCtf18775)

- If the director in the Smart Install network is located between an access point and the DHCP server, the access point tries to use the Smart Install feature to upgrade even though access points are not supported devices. The upgrade fails because the director does not have an image and configuration file for the access point. There is no workaround. (CSCtg98656)

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

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

There is no workaround. (CSCth35152)

**SPAN and RSPAN**

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the **replicate** option. For a remote SPAN session, there is no workaround.

This is a hardware limitation and only applies to these switches (CSCdy72835):

- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS
- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD
- Cisco EtherSwitch service modules

- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the **encapsulation replicate** option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround.

This is a hardware limitation and only applies to these switches (CSCdy81521):

- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS
- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD
- Cisco EtherSwitch service modules

- During periods of very high traffic when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session.

This is a hardware limitation and only applies to these switches (CSCea72326):
- 3560-24PS
- 3560-48PS
- 3750-24PS
- 3750-48PS
- 3750-24TS
- 3750-48TS
- 3750G-12S
- 3750G-24T
- 3750G-24TS
- 3750G-16TD
- Cisco EtherSwitch service modules

- (Catalyst 3750 or 3560 switches and Cisco EtherSwitch service modules) The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: Decreased egress SPAN rate. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded. There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)

- On Catalyst 3750 switches running Cisco IOS Release 12.1(14)EA1 and later, on Catalyst 3560 switches running Cisco IOS release 12.1(19)EA1 or later, or on Cisco EtherSwitch service modules, some IGMP report and query packets with IP options might not be ingress spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)

- Cisco Discovery Protocol (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)
Stacking (Catalyst 3750 or Cisco EtherSwitch service module switch stack only)

- If the stack master is immediately reloaded after adding multiple VLANs, the new stack master might fail. The workaround is to wait a few minutes after adding VLANs before reloading the stack master. (CSCea26207)

- If the console speed is changed on a stack, the configuration file is updated, but the baud rate is not. When the switch is reloaded, meaningless characters might appear on the console during bootup before the configuration file is parsed and the console speed is set to the correct value. If manual bootup is enabled or the startup configuration is deleted after you change the console speed, you cannot access the console after the switch reboots. There is no workaround. (CSCec36644)

- If a switch is forwarding traffic from a Gigabit ingress interface to a 100 Mb/s egress interface, the ingress interface might drop more packets due to oversubscription if the egress interface is on a Fast Ethernet switch (such as a Catalyst 3750-24TS or 3750-48TS switch) than if it is on a Gigabit Ethernet switch (such as a Catalyst 3750G-24T or 3750G-24TS switch). There is no workaround. (CSCed00328)

- If a stack member is removed from a stack and either the configuration is not saved or another switch is added to the stack at the same time, the configuration of the first member switch might be lost. The workaround is to save the stack configuration before removing or replacing any switch in the stack. (CSCed15939)

- When the `switchport` and no `switchport` interface configuration commands are entered more than 20,000 times on a port of a Catalyst 3750 switch or on a Cisco EtherSwitch service module, all available memory is used, and the switch halts.

  There is no workaround. (CSCed54150)

- In a private-VLAN domain, only the default private-VLAN IP gateways have sticky ARP enabled. The intermediate Layer 2 switches that have private VLAN enabled disable sticky ARP. When a stack master re-election occurs on one of the Catalyst 3750 or Cisco EtherSwitch service module default IP gateways, the message `IP-3-STCKYARPOVR` appears on the consoles of other default IP gateways. Because sticky ARP is not disabled, the MAC address update caused by the stack master re-election cannot complete.

  The workaround is to complete the MAC address update by entering the `clear arp` privileged EXEC command. (CSCed62409)

- When a Catalyst 3750 switch or Cisco EtherSwitch service module is being reloaded in a switch stack, packet loss might occur for up to 1 minute while the Cisco Express Forwarding (CEF) table is downloaded to the switch. This only impacts traffic that will be routed through the switch that is being reloaded. There is no workaround. (CSCed70894)

- Inconsistent private-VLAN configuration can occur on a switch stack if a new stack master is running the IP base image and the old stack master was running the IP services image.

  Private VLAN is enabled or disabled on a switch stack, depending on whether or not the stack master is running the IP services image or the IP base image:

  - If the stack master is running the IP services image, all stack members have private VLAN enabled.
  - If the stack master is running the IP base image, all stack members have private VLAN disabled.

  This occurs after a stack master re-election when the previous stack master was running the IP services image and the new stack master is running the IP base image. The stack members are configured with private VLAN, but any new switch that joins the stack will have private VLAN disabled.
These are the workarounds. Only one of these is necessary:

- Reload the stack after an IP services image to IP base image master switch change (or the reverse).
- Before an IP services image-to-IP base image master switch change, delete the private-VLAN configuration from the existing stack master. (CSCee06802)

- Port configuration information is lost when changing from switchport to no switchport modes on Catalyst 3750 switches.
  This is the expected behavior of the offline configuration (provisioning) feature. There is no workaround. (CSCee12431)

- When connected to the router through an auxiliary port in a session to a Cisco EtherSwitch service module, the service module session fails when you enter the shutdown and the no shutdown interface configuration commands on the service module router interface.
  These are the workarounds:
  - Reload the router.
  - Connect to the router through the console port, and open a session to the service module. (CSCeh01250) (Cisco EtherSwitch service modules)

- If one switch in a stack of Catalyst 3750 switches requires more time than the other switches to find a bootable image, it might miss the stack master election window. However, even if the switch does not participate in the stack master election, it will join the stack as a member.
  The workaround is to copy the bootable image to the parent directory or first directory. (CSCei69329)

- When the path cost to the root bridge is equal from a port on a stacked root and a port on a non-stack root, the BLK port is not chosen correctly in the stack when the designated bridge priority changes. This problem appears on switches running in PVST, Rapid-PVST, and MST modes.
  The workaround is to assign a lower path cost to the forwarding port. (CSCsd95246)

- When a stack of 3750 switches is configured with a Cross-Stack EtherChannel and one of the physical ports in the EtherChannel has a link-up or a link-down event, the stack might transmit duplicate packets across the EtherChannel. The problem occurs during the very brief interval while the switch stack is adjusting the EtherChannel for changing conditions and adapting the load balance algorithm to the new set of active physical ports.
  This can but does not always occur during link flaps and does not last for more than a few milliseconds. This problem can happen for cross-stack EtherChannels with the mode set to ON or LACP.
  There is no workaround. No manual intervention is needed. The problem corrects itself within a short interval after the link flap as all the switches in the stack synchronize with the new load-balance configuration. (CSCse75508)

- If a new member switch joins a stack within 30 seconds of a command to copy the switch configuration to the running configuration of the stack master being entered, 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)

- 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)

- 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 if 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) (Catalyst 3750 switches)

- After a stack bootup, the spanning tree state of a port that has IEEE 802.1x enabled might be blocked, even when the port is in the authenticated state. This can occur on a voice port where the Port Fast feature is enabled.
  The workaround is to enter a `shutdown` interface configuration command followed by a `no shutdown` command on the port in the blocked state. (CSCsl64124)

- When a switch stack is running 802.1x single host mode authentication and has filter-ID or per-user policy maps applied to an interface, these policies are removed if a master switchover occurs. Even though the output from the `show ip access-list` privileged EXEC command includes these ACLs, the policies are not applied.
  The workaround is to enter a `shutdown` and then a `no shutdown` interface configuration command on the interface. (CSCsx70643) (Catalyst 3750 switch)

- When the switch stack is in the HSRP active state and a master changeover occurs, you cannot ping the stack by using an HSRP virtual IP address.
  There is no workaround. (CSCsth00938) (Catalyst 3750 and 2960-S switches)

**Trunking**

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber.
  This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface. There is no workaround. (CSCdz33708)
• 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).

• If a Catalyst 3750 switch stack is connected to a designated bridge and the root port of the switch
stack is on a different switch than the alternate root port, changing the port priority of the designated
ports on the designated bridge has no effect on the root port selection for the Catalyst 3750 switch
stack. There is no workaround. (CSCea40988)

• 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)

• (Catalyst 3750 or 3560 switches) A CPUHOG message sometimes appears when you configure a
private VLAN. Enable port security on one or more of the ports affected by the private VLAN
configuration.
There is no workaround. (CSCed71422)

• (Catalyst 3750) When you apply a per-VLAN quality of service (QoS), per-port policer policy-map
to a VLAN Switched Virtual Interface (SVI), the second-level (child) policy-map in use cannot be
re-used by another policy-map.
The workaround is to define another policy-map name for the second-level policy-map with the
same configuration to be used for another policy-map. (CSCef47377)

• When dynamic ARP inspection is configured on a VLAN, and the ARP traffic on a port in the VLAN
is within the configured rate limit, the port might go into an error-disabled state.
The workaround is to configure the burst interval to more than 1 second. (CSCse06827,
Catalyst 3750 switches only)

• 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)

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 36
- Cisco IOS Notes, page 36
- Device Manager Notes, page 37

Switch Stack Notes

- Always power off a switch before adding or removing it from a switch stack.
- Catalyst 3560 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 switches running Cisco IOS Release 12.2(25)SEB are compatible with Cisco EtherSwitch service modules running Cisco IOS Release 12.2(25)EZ. Catalyst 3750 switches and Cisco EtherSwitch service modules can be in the same switch stack. In this switch stack, the Catalyst 3750 switch or the Cisco EtherSwitch service module can be the stack master.

Cisco IOS Notes

- The IEEE 802.1x feature in Cisco IOS Release 12.1(14)EA1 and later is not fully backward-compatible with the same feature in Cisco IOS Release 12.1(11)AX. If you are upgrading a Catalyst 3750 switch running Cisco IOS Release 12.1(11)AX that has IEEE 802.1x configured, you must re-enable IEEE 802.1x after the upgrade by using the `dot1x system-auth-control` global configuration command. This global command does not exist in Cisco IOS Release 12.1(11)AX. Failure to re-enable IEEE 802.1x weakens security because some hosts can then access the network without authentication.
- The behavior of the `no logging on` global configuration command changed in Cisco IOS Release 12.2(18)SE and later. In Cisco IOS Release 12.1(19)EA and earlier, both of these command pairs disabled logging to the console:
  - the `no logging on` and then the `no logging console` global configuration commands
  - the `logging on` and then the `no logging console` global configuration commands
In Cisco IOS Release 12.2(18)SE and later, you can only use the `logging on` and then the `no logging console` global configuration commands to disable logging to the console. (CSCec71490)
- In Cisco IOS Release 12.2(25)SEC for the Catalyst 3750 and 3560 switches and in Cisco IOS Release 12.2(25)SED for the Catalyst 2960 switch, the implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.
- 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:

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ip http authentication</td>
<td>Configure the HTTP server interface for the</td>
</tr>
<tr>
<td>{aaa</td>
<td>enable</td>
</tr>
<tr>
<td></td>
<td>• aaa—Enable the authentication, authorization,</td>
</tr>
<tr>
<td></td>
<td>and accounting feature. You must enter the</td>
</tr>
<tr>
<td></td>
<td>aaa new-model interface configuration command</td>
</tr>
<tr>
<td></td>
<td>for the aaa keyword to appear.</td>
</tr>
<tr>
<td></td>
<td>• enable—Enable password, which is the default</td>
</tr>
<tr>
<td></td>
<td>method of HTTP server user authentication, is</td>
</tr>
<tr>
<td></td>
<td>used.</td>
</tr>
<tr>
<td></td>
<td>• local—Local user database, as defined on the</td>
</tr>
<tr>
<td></td>
<td>Cisco router or access server, is used.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

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 the Catalyst 3750, 3560, 2975, 2960-S and 2960 switches and to Cisco EtherSwitch service modules:

- **CSCur23656** (Catalyst Switch 2960-S, Catalyst Switch 3560, Catalyst Switch 3750)
  Cisco IOS and Cisco IOS-XE (IOSd) include a version of SSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) IDs: CVE-2014-3566
  There is no workaround.

- **CSCte99366**
  In a Smart Install network, when the director is connected between the client and the DHCP server and the server has options configured for image and configuration, then the client does not receive the image and configuration files sent by the DHCP server during an automatic upgrade. Instead the files are overwritten by the director and the client receives the image and configuration that the director sends.
  Use one of these workarounds:
  - If client needs to upgrade using an image and configuration file configured in the DHCP server options, you should remove the client from the Smart Install network during the upgrade.
- In a network using Smart Install, you should not configure options for image and configuration in the DHCP server. For clients to upgrade using Smart Install, you should configure product-id specific image and configuration files in the director.

- **CSCtg35226** (Catalyst 3750 switches)
  Cisco Network Assistant displays the LED ports with a light blue color for all switches in a stack that have the Catalyst 3750G-48PS switch as part of the stack.
  There is no workaround.

- **CSCti30313** (Catalyst 2960, 2960-S, and 2975 switches)
  The output from the `show sdm prefer lanbase-routing` privileged EXEC command shows some incorrect values. The corrected values are:
  - number of IPv4 unicast routes: 4.25K should be: 0.75K
  - number of directly-connected IPv4 hosts: 4K should be: 0.75K
  - number of indirect IPv4 routes: 0.256 should be 16
  There is no workaround.

- **CSCtl77011**
  When port security is enabled on the port, problems arise during web authentication. If the port security violation is set to shutdown mode, the port is error disabled. If the port security violation is set to restrict mode, packets are dropped and an AUTHMGR-5-SECURITY_VIOLATION error is displayed. If the port security violation is set to protect mode, packets are dropped.
  The workaround is to disable port security.

- **CSCtl81217** (Catalyst 3750 and 3560)
  When a switch is using a DHCP server to assign IP addresses and an interface on the switch has RIP enabled, if the switch reloads, the interface loses some RIP configuration (specifically RIP authentication mode and RIP authentication key-chain). This does not happen when the IP address is statically configured on the interface. The problem occurs only when you configure RIP before an IP address is assigned by the DHCP server.
  There is no workaround, but you can use an embedded event manager (EEM) script to add the interface configuration commands on the interface:
  - `ip rip authentication mode`
  - `ip rip key-chain`

- **CSCtn92672** (Catalyst Switch 2960-S)
  In a master and slave fail-over configuration, when the slave client is active, access control lists are downloaded to the switch stack but not installed.
  The workaround is to reboot the stack.

- **CSCto05912** (Catalyst 2960, 2960-S, and 2975 switches)
  When you configure voice and data on the same VLAN, the port is error-disabled during authentication.
  The workaround is to configure voice and data on separate VLANs.

- **CSCto06796**
  When you disable an interface and configure voice and data on the same VLAN and enable the interface:
  - It causes a security violation but voice and data is authorized.
• The configuration for the data VLAN policy changes after authentication. Use the show run interface configuration command to see this.

When you configure voice and data on the same VLAN on an enabled interface, it causes a security violation and an error message is displayed.

In both cases the workaround is to configure voice and data on separate VLANs.

• CSCto25228 (Catalyst Switches 3750, 2960 and 2960-S)

When the show authentication sessions int interface command is entered, the VLAN policy and group information is not displayed. This happens when Open1x is configured on the interface and the DHCP IP address is obtained prior to authentication.

The workaround is to remove the Open1x configuration.

• CSCto99322

If the switch is in multidomain authorization (MDA) mode and it receives three or more MAC addresses simultaneously or if the switch is in single-host mode and it receives two or more MAC addresses simultaneously, a security violation trap occurs in the shutdown and protect violation modes.

The workaround is to connect one device at a time.

• CSCtq06316

If you configure multidomain authentication (MDA) with Open1x authentication and the restrict violation mode, a security violation occurs if the MAC address on the voice LAN is the last MAC address that the switch receives. However, the MAC address is added to the table as a dynamic MAC address and the connected data VLANs continue to access the interface.

The workaround is to connect the voice device first.

• CSCtq06842

In the multidomain authentication (MDA) mode, if you configure the network-policy profile global configuration command and you remove a voice VLAN at the interface level after authentication, tracebacks and error messages are generated.

There is no workaround.

• CSCtq12146 (Catalyst 3560 and 3750 switches)

When MAC authentication bypass (MAB) is configured in single-host mode on the first port and multidomain authentication (MDA) is configured in open authentication mode on the second port, if the MAC Move feature is disabled on the switch, a security violation does not occur when the switch detects the same MAC address on both ports.

The workaround is to manually clear the MAC address table on the second port.

• CSCtw71650 (Catalyst Switches 2960-S and 3750)

In a switch stack where the master switch is running Cisco IOS Release 12.2(58)SE or later and a slave switch is running a release different from the master switch, the auto-upgrade fails and the Cisco IOS configuration is not copied to the slave switches.

The workaround is to remove the slave switches from the stack and manually apply the correct image to the slave switch. Alternatively, use the archive download-sw /overwrite privileged EXEC command to download and install a new image to the switch.

• CSCtx37129 (Catalyst 2960-S and 3750 switches)
If you enter the `shutdown` interface configuration command on the the Fast Ethernet 0 router interface and VLAN 1 client switch interface, and then restart the master switch, the shutdown status of these two interfaces are not shown correctly. If you check their status with the `show running-config` privileged EXEC command, these interfaces are shown as up.

There is no workaround.

## Resolved Caveats

- Caveats Resolved in Cisco IOS Release 12.2(55)SE13, page 41
- Caveats Resolved in Cisco IOS Release 12.2(55)SE12, page 42
- Caveats Resolved in Cisco IOS Release 12.2(55)SE11, page 43
- Caveats Resolved in Cisco IOS Release 12.2(55)SE10, page 44
- Caveats Resolved in Cisco IOS Release 12.2(55)SE9, page 45
- Caveats Resolved in Cisco IOS Release 12.2(55)SE8, page 48
- Caveats Resolved in Cisco IOS Release 12.2(55)SE7, page 49
- Caveats Resolved in Cisco IOS Release 12.2(55)SE6, page 51
- Caveats Resolved in Cisco IOS Release 12.2(55)SE5, page 53
- Caveats Resolved in Cisco IOS Release 12.2(55)SE4, page 56
- Caveats Resolved in Cisco IOS Release 12.2(55)SE3, page 57
- Caveats Resolved in Cisco IOS Release 12.2(55)SE2, page 58
- Caveats Resolved in Cisco IOS Release 12.2(55)SE1, page 59
- Caveats Resolved in Cisco IOS Release 12.2(55)SE, page 61

## Caveats Resolved in Cisco IOS Release 12.2(55)SE13

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvg76186</td>
<td>Cisco Smart Install Remote Code Execution and Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvd40673</td>
<td>Cisco Smart Install Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvd73487</td>
<td>Link Layer Discovery Protocol Buffer Overflow Vulnerability</td>
</tr>
<tr>
<td>CSCuh91645</td>
<td>Cisco IOS and IOS XE Software DHCP Version 4 Relay Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvg62730</td>
<td>Cisco IOS and IOS XE Software DHCP Version 4 Relay Heap Overflow Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvg62754</td>
<td>Cisco IOS and IOS XE Software DHCP Version 4 Relay Reply Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCuu76493</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
<tr>
<td>CSCut50727</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
<tr>
<td>CSCut47751</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
</tbody>
</table>
## Resolved Caveats

### Caveats Resolved in Cisco IOS Release 12.2(55)SE12

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCur29331</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
<tr>
<td>CSCuc53853</td>
<td>Cisco IOS Switch HTTP Server DoS Vulnerability</td>
</tr>
<tr>
<td>CSCvi05126</td>
<td>ISAKMP Notification messages carry unnecessary data</td>
</tr>
<tr>
<td>CSCvg76186</td>
<td>Cisco Smart Install Remote Code Execution and Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvd40673</td>
<td>Cisco Smart Install Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvd73487</td>
<td>Link Layer Discovery Protocol Buffer Overflow Vulnerability</td>
</tr>
<tr>
<td>CSCuh91645</td>
<td>Cisco IOS and IOS XE Software DHCP Version 4 Relay Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvg62730</td>
<td>Cisco IOS and IOS XE Software DHCP Version 4 Relay Heap Overflow Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvg62754</td>
<td>Cisco IOS and IOS XE Software DHCP Version 4 Relay Reply Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCuu76493</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
<tr>
<td>CSCut50727</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
<tr>
<td>CSCut47751</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
<tr>
<td>CSCur29331</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
<tr>
<td>CSCuc53853</td>
<td>Cisco IOS Switch HTTP Server DoS Vulnerability</td>
</tr>
<tr>
<td>CSCvi05126</td>
<td>ISAKMP Notification messages carry unnecessary data</td>
</tr>
<tr>
<td>CSCvd48893</td>
<td>Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability</td>
</tr>
<tr>
<td>CSCto01893</td>
<td>Memory leak observed during SNMPv2c stress testing</td>
</tr>
<tr>
<td>CSCxy56638</td>
<td>Switch crashes after getnext on the last cafServerAliveAction index</td>
</tr>
<tr>
<td>CSCtl42016</td>
<td>Cat3750X Device Manager shows Fan FAULTY if Fan PS is NOT PRESENT</td>
</tr>
<tr>
<td>CSCuw77959</td>
<td>Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability</td>
</tr>
<tr>
<td>CSCsm45390</td>
<td>DHCP relay security vulnerability</td>
</tr>
<tr>
<td>CSCtx35457</td>
<td>Catalyst 3012 Module is missing the product system data in BCT on GUI</td>
</tr>
<tr>
<td>CSCtj06694</td>
<td>2960S Web Gui shows incorrect port stats</td>
</tr>
<tr>
<td>CSCsv51514</td>
<td>Cisco IOS HTTP server vulnerable to CSRF attacks</td>
</tr>
<tr>
<td>CSCvb29204</td>
<td>BenignCertain on IOS and IOS-XE</td>
</tr>
<tr>
<td>CSCve60507</td>
<td>Crash in &quot;mac auth bypass&quot; SNMP code</td>
</tr>
<tr>
<td>CSCuy82078</td>
<td>Cisco IOS and IOS XE Software Layer 2 Tunneling Protocol Denial of Service Vulnerability</td>
</tr>
</tbody>
</table>
Resolved Caveats

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuz47179</td>
<td>Cisco IOS Software for Cisco Industrial Ethernet Switches PROFINET Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCuu13476</td>
<td>Cisco IOS and Cisco IOS XE Software TCP Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvb16274</td>
<td>PPTP Start-Control-Connection-Reply packet leaks router memory contents</td>
</tr>
</tbody>
</table>

Caveats Resolved in Cisco IOS Release 12.2(55)SE11

- CSCtz67345 (Catalyst Switch 2960-S, Catalyst Switch 3560, Catalyst Switch 3750)
  On port with voice vlan and “control direction in” configured, a failed dot1x session is consuming high amount of memory every second resulting in system crash after 2 hours.
  There is no workaround.

- CSCue52167 (Catalyst Switch 3750)
  Switch with the following traceback
  Feb 9 09:00:43.380 PST: %SYS-2-NOBLOCK: idle with blocking disabled.
  There is no workaround.

- CSCuq69695 (Catalyst Switch 2960-S, Catalyst Switch 3560, Catalyst Switch 3750)
  Even though only a certain string match is used in the log filter, also some other non-related logs are being dropped.
  There is no workaround.

- CSCur15364 (Catalyst Switch 3560)
  The status of certain ports is changed to err-disable state.
  There is no workaround.

- CSCut42591 (Catalyst Switch 2960-S)
  High CPU (up to 100%), Device crash, Spanning-tree loop, MAC flaps (on unauth port) symptoms are observed. In addition, when SPAN is configured on unauth port, packets are still captured.
  Workaround is to unconfigure ‘authentication control-direction in’

- CSCuu97954 (Catalyst Switch 3750)
  3750G running 12.2(55)SE3 link isn’t coming up due to auto negotiation problem. Link stays in down (not connected) state. Issue discover during server deployments.
  Workaround is to reload the switch to clear symptoms.
Caveats Resolved in Cisco IOS Release 12.2(55)SE10

- CSCua89434 (Catalyst Switch 2960-S)
  When large bursty traffic is sent on a port, the queue gets stuck and shows a `SUPQ-4-PORT_QUEUE_STUCK` error message.
  There is no Workaround. The switch has to be rebooted to recover.

- CSCtq21722
  When SNMP inform hosts are configured on the switch, the switch may reload when configured for SNMP.
  The workaround is to remove the SNMP host configurations for SNMP informs.

- CSCuo84660
  When updating the running configuration using any type of remote file transfer (via SNMP or copy command), and when the source IP resolves to a DNS hostname longer than 63 bytes, an error message is seen. There is no impact to the system. The running configuration will update as expected.
  The workaround is to copy the file to a local storage first and then copy it from the local storage to the running configuration.

- CSCur53506 (Catalyst Switch 3750)
  When `allowed vlan add/remove` is executed on a `switchport protected` interface, broadcast will be flooded to this interface.
  There is no workaround.

- CSCus52129 (Catalyst Switch 3750)
  A port will remain in a MAB Running state even though the MAC address has been learned on the interface and the device continues to send traffic. This is seen when:
  - switch is running 12.2(55)SE4, 12.2(55)SE8, 12.2(55)SE9
  - the client device is connected to a member switch port.
  - `authentication open` is configured on the port
  - `authentication order mab dot1x` is configured on the port.
  The workaround is to move the port to closed mode to prevent the early learning of the MAC address with `no authentication open`, or change the port to `authentication order dot1x mab`.

- CSCug26848 (Catalyst Switch 3560)
  When Flex links are configured with multicast fast convergence enabled, or IGMPV3 packets are sent by clients connected to the switch, or SVI is configured with IGMPV2, high CPU is seen on the switch running 12.2(55)SE7.
  The workaround is to disable multicast fast convergence.

- CSCtr79958
  When you Telnet or SSH from IPv6 enabled device to IPv6 address on router or switch, or have login success and failure logging enabled, the Login success and failure messages only display the first 32 bits of the IPv6 source address in IPv4 format.
  There is no workaround.

- CSCuo95181 (Catalyst Switch 3750)
With snooping either enabled or disabled, IGMP group specific queries with router alert option are not forwarded by the switch.
There is no workaround.

- **CSCup49030 (Catalyst Switch 3560)**
  If the switch interface is configured with both CDP enabled and port-security enabled, EX90/EX60 cannot get IP via DHCP in the data VLAN (EX configured not to use voice vlan).
The workaround is to disable one of the following:
  - Port-security
  - CDP on the interface
  - Voice Vlan on the interface

- **CSCur73813 (Catalyst Switch 3750)**
  On a full-duplex mode, the deferred of show command is "0", but SNMP of `dot3StatsDeferredTransmissions` is not "0", instead it shows the same value with output drops.
There is no workaround.

- **CSCun69150 (Catalyst Switch 2960-S)**
  When the switch is in a network where Layer 2 Protocol Tunneling is configured, the Layer 2 Protocol Tunneling packets are not forwarded by the switch.
The workaround is to use 2960 switch instead of 2960S, as 2960 switches are not affected.

- **CSCui83823**
  When `term length 0` is enabled, the putty session closes prematurely while executing `show tech` or any show commands which gives a long output.
The workaround is to redirect the output to a file.

### Caveats Resolved in Cisco IOS Release 12.2(55)SE9

- **CSCsh15817**
  IP Service Level Agreement operations on a router that also has a response time reporter (RTR) enabled on it, fails at the source. This happens because the RTR responder does not receive the UDP socket events when a UDP packet is routed through a VRF.
The workaround is to use IP SLA operations without VRFs.

- **CSCtg91847 (Catalyst Switches 2960, 2960-S, 2960-SM, 3560, and 3750)**
The switch fails while running 802.1X configuration.
There is no workaround.

- **CSCtr38563**
  Switch fails when a secondary IP address is configured on a VLAN interface.
There is no workaround.

- **CSCtr16643 (Catalyst Switches 2960-S and 2960-SM)**
  Access Control List (ACL) with deny access control entries appear on the switch virtual interface even though the switch does not deny traffic.
Resolved Caveats

The workaround is to remove the **no ip unreachables command** from the switch virtual interface to stop the messages.

- CSCuc63146
  Port-channel interface flaps while adding or removing a VLAN from the trunk on a port-channel interface if one or more port members are not in P or D states.
  The workaround is to shut down the port members which are not in P or D states and make the VLAN changes.

- CSCuh43252
  After upgrading to Cisco IOS Release 15.0(2)SE3, the switch does not authenticate using TACACS.
  The TPLUS process on the switch pushes the CPU usage up to 99%.
  The workaround is to downgrade the switch software to a version prior to Cisco IOS Release 15.0(2)SE3.

- CSCui13971 (Catalyst Switches 2960, 2960-S, 2960-SM, 3750, and 3750V2)
  When 802.1X protocol is configured on a switch stack, the authentication protocol works on master switch but does not work on the stack members.
  The workaround is to run the show command followed by the no show command on the switch.

- 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.

- CSCuj54648
  A malformed TCP packet forwarded on a STP blocked port keeps looping in the network even after traffic is stopped, creating CPU hogs on switches.
  To stop the loop and flooding in the network use one of these workarounds:
  - Run the **shutdown** command followed by the **no shutdown** command on any port in the topology.
  - Change the STP priority of any of the switches.

- CSCuj77254 (Catalyst Switches 2960, 2960-S, 2960-SM, 3560 and 3750)
  Access Control List (ACL) configured on guest VLAN interface for 802.1X unauthenticated clients do not get applied.
  The workaround is to configure the ACL on the dot1x port itself instead of the guest VLAN interface.

- CSCuj77426 (Catalyst Switches 2960, 2960-S, and 3560)
  After running the **shutdown** command followed by the **no shutdown** command on the switch, few ports go into not connected state even though these are connected to a remote device.
  The workaround is to run the **shutdown** command followed by the **no shutdown** command on the affected ports.

- CSCtu04164 (Catalyst Switch 2960-S)
  The **udd aggressive** global command enables unidirectional link detection on copper ports.
Resolved Caveats

There is no workaround.

- **CSCtx37546**
  After stack switchover **length 0** automatically gets set to **line vty** on stack master or member.
  There is no workaround.

- **CSCua69378** (Catalyst Switches 3750V2 and 3560V2)
  When Flex Link is configured on stacks containing interfaces from different switches, the interfaces start flapping continuously.
  The workaround is to remove the Flex Link configuration from the interfaces.

- **CSCsv29870**
  When Routing Information Protocol (RIP) is configured and **clear ip route** command is run on the switch, the RIP sends multiple requests for each interface instead of one request.
  There is no workaround.

- **CSCud19122** (Catalyst Switches 2960, 2960-S, and 2960-SM)
  When **shutdown** command followed by **no shutdown** command is run on a Small Form-Factor Pluggable (SFP) switch interface with full-duplex configured on it, the duplex status changes to half.
  The workaround is to delete the duplex configuration and configure again.

- **CSCue09838** (Catalyst 2960CG switch)
  When **show tech** command is run on the switch through Telnet, the VLAN halts.
  The workaround is to reload the switch.

- **CSCue92168** (Catalyst Switch 2960-S)
  When Quality of Service (QoS) is enabled in a switch stack, the traffic is disrupted.
  The workaround is to reload the switch.

- **CSCue94493**
  When Cisco IP Communicator (CIPC) is turned on and the Cisco Discovery Protocol (CDP) is enabled on the switch, the MAC address of CIPC incorrectly appears in the voice VLAN.
  The workaround is to disable CDP on Cisco IP Communicator.

- **CSCug51225** (Catalyst Switches 2960-S and 3750)
  When a new member is added to the switch stack, it triggers a Topology Change Notification (TCN) flood over the network.
  There is no workaround.

- **CSCuh80308**
  When Access Control List (ACL) entries are applied to the switch interface using **copy tftp: running-config** command, it stops forwarding fragmented traffic.
  Use one of the following workarounds:
  - Apply the ACL configuration through CLI.
  - Remove the ACL from the interface and apply again through the CLI.
  - In the ACL specify the traffic using IP addresses.

- **CSCsw43080**
  For Cisco IOS Releases earlier than 12.4(24)T, traceback and **%DATACORRUPTION-1-DATAINCONSISTENCY** errors are observed in the log.
Resolved Caveats

There is no workaround.

- CSCuh72558
  In a switch stack, if a stack member is connected to a Meru access point that requires 802.3at or 29.5W POE+ inline power, connection over 802.3at POE+ fails.
  The workaround is to move all affected POE+ devices to the stack master.

- CSCui56736
  This issue is seen on Cisco IOS Releases 12.2(55)SE and later, 12.2(58)SE and later, and 15.0(2)SE and later. When the switch stack is reloaded, configuration is initialized, the vlan.dat file is deleted, and VTP version 3 is configured, the `show vtp status` command gives inconsistent results on the stack master and member switches. When the command is run on the stack master, the stack master is shown as server in the VLAN and transparent in the Multiple Spanning Tree (MST) instance. But when the command is run on a member switch, the member switch is shown as the primary server for both the VLAN and the MST instance. When the `vtp mode transparent mst` command is entered, the `Device mode already VTP Transparent for MST message is displayed. Now if the master switch is reloaded, the whole stack is shown as the primary server for both the VLAN and the MST.
  The workaround is to change the VTP version to 2 and then change it back again to 3.

- CSCtd62339
  The following error is seen when EIGRP is enabled on the switch: `%EIGRP: Failed to get client handle from BFD`
  There is no workaround.

- CSCti88809
  If Smart Install is enabled and the `shutdown` command is entered on a range of interfaces followed by the `no shutdown` command, a traceback is seen due to data corruption.
  The workaround is to disable Smart Install by entering the `no vstack` global configuration command.

- CSCtr24525
  The value of the `logmessageperiod` command in the Precision Time Protocol (PTP) announce packet shows the erroneous value of 127.
  There is no workaround.

Caveats Resolved in Cisco IOS Release 12.2(55)SE8

- CSCtf23298
  When a Terminal Access Controller Access Control System (TACACS) server is configured with a single connection, the CPU usage is high.
  The workaround is to remove the single connection option.

- CSCtt19737
  Cisco IOS IP SLAs probes fail because the control message is blocked. The firewalls block the control message when a response packet is not returned to the originating port.
  The workaround is to disable IP SLAs control messages for this probe instance.

- CSCty66157
  The `snmp-server group` command does not associate both IPv6 and IPv4 ACLs simultaneously with an SNMP group.
Resolved Caveats

The workaround is to use the `snmp-server user` command, which associates both IPv4 and IPv6 ACLs with an SNMP user.

- **CSCub93357** (Catalyst Switches 2960, 2960-S, 2960-SM and 3750)
  After configuring switch port security using the `switchport port-security maximum 1 vlan access` command, if an IP phone with a personal computer connected to it is connected to the same access port, the switch displays the following error message:

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address XXXX.XXXX.XXXX on port <interface>
  ```

  There is no workaround.

- **CSCuc10143** (Catalyst Switches 2960-S, 2960-SM, 3560, 3560-LM, 3750 and 3750-LM)
  In the event of a power supply failure in the Redundant Power System (RPS) 2300 connected to a switch, the switch sends continuous traps with RPS states alternating between RPS unknown and RPS normal.
  
  The workaround is to disconnect the RPS from the switch in the event of a power failure. This helps to prevent the traps.

- **CSCuc95754** (Catalyst Switch 2960-S)
  Port ASIC's TCAM test fails when executing on-demand diagnostic tests using the diagnostic start command.
  
  The workaround is to ignore the results of on-demand diagnostic tests, if Power-On Self-Test (POST) at bootup succeeds.

- **CSCud79753**
  When a switch is configured with Cisco IOS IP SLAs FTP GET operation and if the target file is unavailable, the switch experiences a memory leak and may become unresponsive if it runs out of memory.
  
  The workaround is to configure the Cisco IOS IP SLAs FTP GET operation only after verifying the availability of the remote target file and setting the permissions for the file, as appropriate. This allows the switch to retrieve the file and not experience a memory leak.

- **CSCue07405**
  When manually running on-demand diagnostic tests on a stack member using the `diagnostic start switch number test all` interface configuration command, the test `TestPortAsicRingLoopback` fails arbitrarily.
  
  The workaround is to run only the `TestPortAsicRingLoopback` test (`diagnostic start switch number test 4` interface configuration command) on the stack member. Isolate the stack member and then run the `diagnostic start switch number test all` interface configuration command on the rest of the stack.

- **CSCue54767** (Catalyst Switches 2960, 3560 and 3750)
  Packet fragments in the TCP header field are dropped when transmitting for a SPAN session.
  
  There is no workaround.

## Caveats Resolved in Cisco IOS Release 12.2(55)SE7

- **CSCtg52885**
  The Hot Standby Router Protocol (HSRP) on dot1q sub-interfaces remains in INIT state after a physical link flap on the trunk port.
Resolved Caveats

The workaround is to enter the `shutdown` and `no shutdown` command on the interface.

- **CSCtz96168**
  IPv6 packets travel randomly between two isolated ports that are in the same VLAN.
  There is no workaround.

- **CSCua54224 (Catalyst Switch 3750)**
  If several interfaces on the stack (35 to 40 or more) flap at the same time, loop guard is activated and the root port is blocked and unblocked. The following error message is displayed:
  
  `%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet1/0/1 on MST0.`
  `%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet1/0/1 on MST0.`
  
  There is no workaround.

- **CSCub04965 (Catalyst Switch 3750)**
  Cisco Catalyst 3750 v1 switches that run Cisco Secure Access Control Server (ACS) show erratic behavior, exhibiting one or more of the following characteristics:
  
  - Packet data is lost when a device pings the switch. This loss is initially about 20 percent, and progressively increases until the switch stops passing data altogether.
  - Packet data is lost when a directly connected device pings the loopback address of the switch. This loss is again about 20 percent.
  - The following error message is displayed when you run a command: `Command authorization failed`. If you run the command again, it is executed successfully.

  The workaround is to remove authentication, authorization, and accounting (AAA) and clear the TCP sessions. Alternatively, downgrade to Cisco IOS Release 12.2(35)SE.

- **CSCub92642**
  If the switch is configured with Multicast Distributed Switching (MDS), memory leaks if the `multicast-routing distributed` command is toggled repeatedly.
  There is no workaround.

- **CSCuc48628 (Catalyst Switch 3750)**
  If a Cisco Catalyst 3750-X switch is added to a Catalyst 3750 switch stack, the member switch upgrade fails and the bootable image may be deleted from the member switch's flash memory. This issue is seen if the version of the switch stack does not match with the version of the member switch.
  
  Perform one of the following tasks for the workaround:
  
  - Specify the correct image file in the auto-download option. For example, enter the `boot auto-download-sw tftp://tftp_ip_address/c3750e-version.tar` global configuration command.
  - If the 3750-X member switch contains the .tar image file for an older 3750 switch, delete this .tar file before adding the switch to the stack.
  - Check if the software image .bin file has been copied to the root directory of the 3750-X switch, and reload the switch.

- **CSCuc85964 (Catalyst Switches 3750 and 3750-G)**
  If a mixed switch stack is reloaded, the MAC address table does not synchronize between the master and the member switches.
  
  The workaround is to run the `clear mac address-table dynamic` privileged EXEC command when the switch is reloaded and traffic starts flowing.
Resolved Caveats

- CSCud17778
  Memory leaks (due to SNMP traps) cause the switch to respond slowly to commands; eventually the switch fails. This is observed when more than one SNMP server host is configured, one of the host broadcasts SNMP traps, or the `snmp-server enable traps snmp authentication coldstart warmstart` command is configured.
  
The workaround is to disable the `snmp-server enable traps snmp authentication coldstart warmstart` command and reload the switch.

- CSCud21309 (Catalyst Switch 3750 and 3560)
  In a private VLAN, isolated ports leak ARP packets when port-based authentication is enabled.
  There is no workaround.

Caveats Resolved in Cisco IOS Release 12.2(55)SE6

- CSCef01541
  The switch processes data packets that are sent to the network address of an interface if the layer-2 frame encapsulating that packet is specifically crafted to target layer-2 address of the interface or a broadcast layer-2 address.
  
The workaround is to use Cisco Express Forwarding (CEF).

- CSCtk18810
  High memory usage is seen with the 'Virtual Exec" process.
  There is no workaround.

- CSCto57723
  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.
  
  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6

- CSCtr32202 (Catalyst Switch 2960-S)
  Multicast VLAN Registration does not work as expected across a switch stack.
  
The workaround is to use normal Internet Group Management Protocol (IGMP) snooping across the stack.

- CSCtt31901
  The `sh udld neighbor` command does not work.
  
The workaround is to enable the `udld port aggressive` command on the interface level once.

- CSCtw58495
  The switch stops working when you enter the `show epm session summary` privileged EXEC command.
  
  There is no workaround.

- CSCtx20903
Resolved Caveats

In a single connection-enabled Terminal Access Controller Access Control System (TACACS) server, when the primary TACACS server goes down, the authentication fallback to the secondary server fails.

The workaround is to disable the single connection.

- CSCtx47330 (Catalyst Switches 2960-S and 3750)
  The Gigabit Ethernet port on the switch stack does not work when several ports are in the link up state.
  There is no workaround.

- CSCtx61557
  The switch stops working even after a successful 802.1x authentication of the client.
  There is no workaround.

- CSCtx90729 (Catalyst Switch 2960-S)
  The switch hangs at "POST: Thermal, Fan Tests : Begin" during boot after power was previously lost during the front-end microcode update portion of a Cisco IOS upgrade. Thereafter, the switch hangs on all subsequent attempts to recover through reload.
  The workaround is to recover the switch by bringing it to its boot loader prompt using the corrupted or missing image recovery procedure. Alternatively, boot the Cisco IOS image to recover or load a Cisco IOS image with Xmodem.

- CSCtx96491
  A port configured and authenticated with 802.1x security may not correctly detect a loop even if the Bridge Protocol Data Unit (BPDU) guard is configured on the interface. This may result in 100 percent CPU utilization because of the Spanning Tree Protocol (STP) process of the switch.
  The workaround is to configure the switch with the authentication open or authentication mac-move permit command.

- CSCtx99483
  The switch reloads unexpectedly due to segV exception while making PBR configuration changes.
  There is no workaround.

- CSCty93544
  Traffic that should be dropped or denied by an Access Control List (ACL) is permitted by the switch.
  The workaround is to remove and reapply the ACL.

- CSCty98117 (Catalyst Switch 2960-S)
  The switch fails to apply an auto smartport macro after being reloaded.
  The workaround is to enter and exit the configuration mode. Alternatively, enter the sh running-config command.

- CSCtz27507
  When a switch is configured for SNMP and receives SNMP packets from an authenticated user, a successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended Denial of Service (DoS) condition.
  There is no workaround.

- CSCtz92782
  Advanced Access Control List (dACL) does not get applied to a switch interface configured for Multi-Domain Authentication (MDA).
The workaround is to modify the dACL name and configuration.

- CSCua09639
  ARP is blocked with open authentication-enabled switch ports.
  The workaround is to run the command **clear authentication session**.

## Caveats Resolved in Cisco IOS Release 12.2(55)SE5

- CSCsy43147
  During a Telnet session, the router crashes when the TACACS+ server is configured or unconfigured (**tacacs-server host** command) using the **single-connection** keyword.
  The workaround is to not use the **single-connection** keyword.

- CSCtb35715
  When you enter the **show running-config** interface configuration command, IP Service Level Agreement notifications are shown as enabled even when you have not enabled this configuration using the **ip sla enable reaction-alerts** interface configuration command.
  There is no workaround.

- CSCtc18841
  If local proxy Address Resolution Protocol (ARP) is configured on the VLAN interface, the ARP entry for the Hot Standby Router Protocol (HSRP) enters into an incomplete state.
  The workaround is to remove the proxy ARP feature on the VLAN interface (by using the **no ip local-proxy-arp** interface configuration command) and restart the interface.

- CSCtc56652 (Catalyst Switch 2960-S)
  The switch fails when you enter the **debug platform cpu-queues** privileged EXEC command. The problem occurs because the contents of the packet's **pak->rx_descriptor** pointer have been overwritten, and the pointer is therefore invalid.
  The workaround is to move the 24 bytes of the **pak->rx_descriptor** pointer to another memory location before the start of the MAC address header. Because the data area before the MAC address header is now unused, there will not be any overwrites and the packet realign will occur smoothly.

- CSCtg38468
  When AAA authorization is used with TACACS+, an error is displayed if the banner message (**banner exec** global configuration command) starts with a blank character.
  The workaround is to not start the banner message with a blank character.

- CSCth00398
  If the **no vtp** VLAN configuration command is used on a port that receives VTP updates, the switch does not process Layer 2 control traffic (STP and CDP) after some time.
  The workaround is to configure VTP on the port or to not use the **no vtp** command.

- CSCtj22354
  The switch fails when LLDP data units with Type Length Value (TLV) of more than 10 management addresses (MA) are received.

- CSCtj89743
CPU usage is high when a device connected to the switch is accessed using the `https://IP_address` command on the router.

The workaround is to reload the device.

- **CSCtj95182 (Catalyst Switches 2960, 3550, 3560, and 3750)**
  If a network scanner is used to check the network components, a memory leak occurs in the SMI IBC/IBD server process, and the CPU load is unusually high.
  There is no workaround.

- **CSCtk12589 (Catalyst Switch 2960)**
  The following error message is displayed several times when you boot the switch. The switch functionality is not hampered, and the switch continues to operate normally after booting.
  ```
  Yeti2S88gMdioWr: Unknown status for write operation
  ```
  The workaround is to restart the switch.

- **CSCtn10697**
  The switch crashes when DCHP snooping is enabled with value 125 and an offer packet is received.
  There is no workaround.

- **CSCto72927**
  If a Tcl policy is copied to the router, the router fails when an event manager policy is configured.
  There is no workaround.

- **CSCtq09233**
  If a CLI configuration text file is copied from a Windows system to the switch, a space is appended to the end of the macro description command when the file is read from the flash of the switch. This leads to errors resulting in high CPU utilization on the switch. Another possible issue is that the macro is not removed when the link goes down or the connected device is removed from the switch.
  The workaround is to copy the configuration file from a non-Windows system (like UNIX or Linux) or convert the file to an appropriate UNIX format before copying.

- **CSCtq72873 (Catalyst Switches 3560 and 3750)**
  In this race condition, the switch fails when a MAB client fails to authenticate on the switch (possibly caused by the ACS server being unavailable) and the client is simultaneously deleted from the switch (possibly by entering the `clear authentication sessions` privileged EXEC command).
  There is no workaround. The risk of switch failure can be minimized by ensuring that MAB-enabled interfaces are not shut down and that commands that clear the MAB sessions are avoided.

- **CSCtr28857**
  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.
  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

- **CSCtr55645 (Catalyst Switches 3560 and 3750)**
  IPv6 multicast packets for routing protocols (such as OSPFv3 hello messages) are not enqueued to CPU queue 3 as expected.
Resolved Caveats

- **CSCtr79337 (Catalyst Switch 2960-S)**
  When switch ports operate at 100-Mbps or 10-Mbps Ethernet speeds with half-duplex auto-negotiation, connectivity is erratic on the ports.
  The workaround is to configure the ports to use full-duplex auto-negotiation.

- **CSCtr87729 (Catalyst Switch 3750)**
  The stack member switch MAC address table does not synchronize correctly after reload.
  The workaround is to reload the channel interface using the `shutdown` interface configuration command followed by the `no shutdown` command. Alternatively, clear the MAC address table.

- **CSCtr91106**
  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.
  Products that are not running Cisco IOS Software are not vulnerable.
  Cisco has released free software updates that address these vulnerabilities.
  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.
  This advisory is available at the following link:

- **CSCts34688**
  The switch crashes due to the "HACL Acl Manager" memory fragmentation when a large access control list (ACL) is modified.
  The workaround is add or remove ACE entries in sequential order when the ACL is modified.

- **CSCts56125 (Catalyst Switch 3560)**
  When a switch powers on and none of the ports are up, the switch reloads in 15 minutes if it cannot contact the TACACS+ server.
  The workaround is to not use the broadcast keyword in the TACACS+ server configuration.

- **CSCts58073 (Catalyst Switches 2960, 3560, and 3750)**
  A threshold violation error message is displayed when a X2-10GB-LR module is installed on the switch (with or without a fiber cable). An example error message is:
  `SFP8472-5-THRESHOLD_VIOLATION: Te1/0/1: Voltage low alarm; Operating value: 0.00 V, Threshold value: 2.96 V`
  There is no workaround.

- **CSCts75641**
  Routing Information Protocol (RIP) Version 2 packets egressing an 801.1Q tunnel interface are triplicated.
  There is no workaround.

- **CSCtt16051**
  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.
Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

- **CSCtt37202**
  
  If a client switch is authorized using MAC Authentication Bypass (MAB), and then by using the 802.1x standard and dynamic VLAN assignment, the MAC address of the switch is not updated in the MAC address table of slave switches.

  The workaround is to not use both the 802.1x and dynamic VLAN assignment configurations for the client switch.

- **CSTu17483**
  
  The switch crashes when an IP phone that uses LLDP and authenticates itself using MAC Authentication Bypass (MAB) or 802.1x is physically disconnected and reconnected to the switch port.

  The workaround is to remove the `aaa authorization network default group SG-PBA` global configuration command.

### Caveats Resolved in Cisco IOS Release 12.2(55)SE4

- **CSCta85026**
  
  The Dynamic Host Configuration Protocol (DHCP) CLI does not accept white spaces in raw ASCII option in the DHCP pool configuration submode. This issue is seen in Cisco IOS Release 12.4(24)T1 and later.

  There is no workaround.

- **CSTg11547**
  
  In a VPN Routing and Forwarding (VRF) aware setup, messages are not sent to the syslog server. This issue applies to Cisco IOS Release 12.2(53)SE and 12.2(53)SE1. This situation does not occur if system logging is configured in the global table.

  This problem has been corrected.

- **CSCth03648 (Catalyst Switches 2960-S)**
  
  When two traps are generated by two separate processes, the switch fails if one process is suspended while the other process updates some variables used by the first process.

  The workaround is to disable all SNMP traps.

- **CSCth87458**
  
  A memory leak occurs in the SSH process, and user authentication is required.

  The workaround is to allow SSH connections only from trusted hosts.

- **CSCth92116**
  
  The log message “Invalid packet (too small) length=0” is displayed when a packet’s destination port is udp 2228.

  There is no workaround.
• CSCti37197
  If a tunnel interface is configured with Cisco Discovery Protocol (CDP), the switch fails when it receives a CDP packet.
  The workaround is to disable CDP on the interface by using the `no cdp enable` interface configuration command.

• CSCtj56719
  The switch fails when the Differentiated Services Code Point (DSCP) mutation name is longer than 25 characters.
  The workaround is to configure DSCP mutation names with fewer than 25 characters.

• CSCtj83964 (Catalyst Switches 3750 and 3560)
  On a switch running Protocol-Independent Multicast (PIM) and Source Specific Multicast (SSM), multicast traffic might not be sent to the correct port after the switch reloads.
  The workaround is to enter the `clear ip route` privileged EXEC command or reconfigure PIM and SSM after a reload.

• CSCtl60151
  The switch sometimes reloads after a CPU overload, regardless of the process that is overloading the CPU.
  This problem has been corrected.

• CSCtn11259 (Catalyst Switch 3750)
  If a switch stack is configured with the `stack-mac persistent timer value` interface configuration command, the switch virtual interface (SVI) should remain in shutdown mode during a switchover. In this case, the SVI is in up mode.
  The workaround is to specify the timer value to be long enough so that the stack’s MAC address is not changed.

• CSCtr79386
  The switch fails when DHCP snooping is configured and packet data traffic is excessive. The traffic exhausts the I/O memory and triggers the switch to crash.
  There is no workaround.

Caveats Resolved in Cisco IOS Release 12.2(55)SE3

• CSCtn72916 (Catalyst Switch 2960-S)
  If you are using a GLC-FE-100FX SFP module on the WS-C2960S-24TS-S model that is running Cisco IOS Release 12.2(55)SE2, the port channel is in half-duplex mode even though member links are in full-duplex mode.
  The workaround is to configure the same command for the port channel and the member links. Use either the `duplex full` interface configuration command or the `no duplex` interface configuration command.

• CSCto10165
  A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.
  Cisco has released free software updates that address this vulnerability.
Resolved Caveats

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


- CSCt046868

If you configure multidomain authentication (MDA) with Open1x authentication and the restrict violation mode, only two MAC addresses are allowed to access the interface. A security violation occurs when a third MAC address on a voice VLAN tries to access the interface. The voice VLAN is not authenticated, and a syslog message is generated. However, the MAC address is not removed from the voice VLAN because Open1x authentication is configured. If you have authorized the voice VLAN with a policy, such as a dynamic VLAN, the policy is not applied.

The workaround is to not configure a voice VLAN on the phone.

- CSCt055124

When a member switch port security is used with port-based dot1x authentication and the switch MAC address is sticky, a connected device authenticates itself. Its MAC address is added as sticky in the switch configuration and in the port security tables of the stack switches. When the switch is shut down, the device MAC address is removed from the master switch, but it is retained in the member switch security tables. When the interface is re-enabled, the device MAC address is restored to the master switch configuration.

The workaround is to use port security without dot1x authentication.

Caveats Resolved in Cisco IOS Release 12.2(55)SE2

- CSCsu74220 (Catalyst Switch 2960-S)

When you filter system messages to a buffer or host, the log output appears incorrectly.

There is no workaround.

- CSCtd10712 (Catalyst Switch 2960-S)

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.


- CSCtk83770 (Catalyst Switch 2960-S)

On the Catalyst 2960-S switch, the fallback pool buffer is 8 bytes smaller than the regular pool buffer. When there is high CPU traffic, the regular buffers are reserved for processing. Applications then use the fallback pool. Because the fallback pool is smaller, a switch stack can fail.

The workaround is to upgrade to Cisco IOS version 12.2(55)SE2 or later.
Caveats Resolved in Cisco IOS Release 12.2(55)SE1

- **CSCtb77390 (Catalyst Switch 2960-S)**
  The SFP+ module PID appears incorrectly in the `show inventory` privileged EXEC command.
  The workaround is to get the correct PID from the SFP+ module label.

- **CSCtc91312 (Catalyst Switches 3750, 3560 and 2960)**
  EnergyWise is enabled and you use the `energywise level level recurrence importance importance at minute hour day_of_month month day_of_week` interface configuration command to configure a recurring event on a switch. After the time changes from daylight savings time to standard time, the switch might
  - Restart when it tries to power a PoE device
  - Power on or off the PoE device at an incorrect time
  - Fail
  This occurs when the time change for the next year occurs after the time change for the current year.
  Before the time change occurs, use one of these workarounds:
  - Remove the recurring events from the EnergyWise configuration, do not use recurring events for a week, and reconfigure them a week after the time change occurs.
  - Use the `energywise level level recurrence importance importance time-range time-range-name` interface configuration command to reschedule the events.
  - Use the `power inline auto` interface configuration command to power on the PoE port.

- **CSCtf30566 (Catalyst Switches 3750 and 3560)**
  A 3750 switch fails when both voice and data VLAN are statically configured as VLAN 1 and an authentication takes place (phone connection or automatic re-authentication). The switch does not fail if voice and data VLANs are assigned dynamically through the Access Control Server (ACS), even if they are configured as VLAN 1.
  There is no workaround.

- **CSCtg04649 (Catalyst Switches 3750 and 2960)**
  When auto negotiation is not used, you cannot manually change the duplex setting on any interface, even if the interface command is successful and the switch enters the command in the configuration. The switch interface continues to operate at the old duplex value.
  The workaround is to enable auto negotiation on the switch interface and then manually set the desired duplex value. Alternatively, enter the `shutdown` and then the `no shutdown` interface configuration command. This sets the duplex value as specified in the interface configuration.

- **CSCth03549 (Catalyst Switches 3750V2 and 3560V2)**
  Catalyst 3560v2 and 3750v2 switch upgrades or downgrades take significantly longer than those for non-V2 switches.
  There is no workaround.

- **CSCth50169 (Catalyst Switch 3750)**
  When you use a switch in a stack running Cisco IOS Release 12.2(55)SE or earlier, it stops working randomly while resolving the Address Resolution Protocol (ARP).
  The workaround is to enable IP routing and add a static ARP for the default gateway:
  ```
  Switch(config)#arp <gateway IP address> <MAC address> arpa
  ```
Resolved Caveats

- CSCth50601 (Catalyst Switch 3750)
  In a mixed stack of Catalyst 3750 and 3750-E switches running Cisco IOS Release 12.2(53)SE, a Catalyst 3750-E switch is not elected as the stack master even if it has a higher priority than a Catalyst 3750 switch.
  The workaround is to start the Catalyst 3750-E switch, and after it is up, start the rest of the switches.

- CSCth62692 (Catalyst Switches 2960 and 2960-S)
  The ip igmp option is missing in the command line interface subcommand query help, accessed by entering ? after the configure terminal interface interface-id # prompt. When you enter ip ? in interface configuration mode, the igmp keyword does not appear, even though the igmp subcommands and functionality, such as ip igmp filter and igmp snooping, are available on the interface.
  There is no workaround.

- CSCti30070 (Catalyst Switches 3750, 3560 and 2960)
  If the status of the AAA server is DEAD and you configure MAC Authentication Bypass (MAB), the client is authorized in the critical VLAN state but the ARP request for the client gateway is not resolved. To check the status of the AAA server, enter the show aaa servers privileged EXEC command.
  There is no workaround.

- CSCti69845 (Catalyst Switches 3750, 3560 and 2960)
  When MAC Authentication Bypass (MAB) is used in multi-authentication mode, a security violation occurs after successful authentication.
  The workaround is to use a different authentication mode (single, multidomain or multihost).

- CSCti61070 (Catalyst Switches 3750 and 2960-S)
  In a switch stack running Cisco IOS Release 12.2(52)SE, the master switch does not join the stack if there is live traffic between the master and member switches.
  There is no workaround.

- CSCti72424 (Catalyst Switches 3750, 3560 and 2960)
  When you enter the aaa accounting send stop-record authentication failure global configuration command on the switch to refine authentication and enable the authentication manager process, the switch might experience a memory leak. This can occur on switches when 802.1x and MAC authentication bypass are enabled, and both authentication attempts fail and then succeed. If the client is then removed from the interface when the port shuts down or the client logs off, the memory leak occurs every time the client is reattached.
  The workaround is to enter the no aaa accounting send stop-record authentication failure to disable the process.

- CSCti01638
  After you upgrade to Cisco IOS Release 12.2(55)SE, port security might not work properly, and the ports might not come online.
  There is no workaround

- CSCti03875 (Catalyst Switches 3750, 3560 and 2960)
  When you disconnect the spanning tree protocol (STP) peer link, the STP port path cost configuration changes.
  There is no workaround.
Resolved Caveats

- **CSCtj11377** (Catalyst 2960-S switch)
  On a Catalyst 2960-S switch, removing QoS or ACL commands from an interface does not always clear the hardware TCAM entries, which could result in traffic loss or unexpected behavior of the switch.
  There is no workaround. Reloading the switch might temporarily resolve the issue, but it could reoccur.

- **CSCtj30297** (Catalyst Switches 3750, 3560 and 2960)
  In a stacked or standalone switch with 32 switch virtual interfaces (SVIs), the system might reload unexpectedly during a network scan using a third-party tool. This does not happen in a switch with just one SVI.
  There is no workaround.

- **CSCtj30652** (Catalyst Switch 2960-S)
  A stack of Catalyst 2960-S switches that are connected to a distribution switch through an EtherChannel might experience frequent STP root changes or STP topology changes without a physical STP loop.
  The workaround is to implement the stack in a half-ring topology instead of a full-ring topology.

- **CSCtj86299**
  If a static MAC address entry is configured for an IP address in the global routing table, ping requests are sent through the global context, and replies are sent through Virtual Routing and Forwarding (VRF). This is a VRF leak.
  The workaround is to remove the static MAC address entry.

Caveats Resolved in Cisco IOS Release 12.2(55)SE

- **CSCeh52964** (Cisco EtherSwitch service modules)
  When the router is rebooted after it is powered on (approximately once in 10 to 15 reboots), the Router Blade Communication Protocol (RBCP) between the router and the EtherSwitch service module might not be reestablished, and this message appears:

  \[date\]: %Y88E8K-3-ILP_MSG_TIMEOUT_ERROR: GigabitEthernet1/0: EtherSwitch Service Module RBCP ILP messages timeout

  The workaround is to reload the EtherSwitch service module software without rebooting the router. You can reload the switching software by using the `reload` user EXEC command at the EtherSwitch service module prompt or by using the `service-module g slot_number /0 reset` privileged EXEC command at the router prompt.

- **CSCsg91027**
  When the `logging event-spanning-tree` interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the `logging event-spanning-tree` interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

  High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

  Use one of these workarounds:
- Disable logging to the console.
- Rate-limit logging messages to the console.
- Remove the logging event spanning-tree interface configuration command from the interfaces.

- **CSCsu31853** (Catalyst Switches 3750, 3560, 2960-S, and 2960)
  The buffer space of a switch running TCP applications is full while the TCP sessions are in the TIME_WAIT state. Buffer space becomes available after the TCP session the closed.
  There is no workaround.

- **CSCsx38711** (Catalyst Switch 3750)
  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.

- **CSCtb08823** (Catalyst Switch 3750)
  SNMP requests on the stpxRSTPPortRoleTable object only return information for the stack master.
  There is no workaround.

- **CSCtb12209**
  When port security is configured to restrict data on a port when a violation occurs, it can interfere with Spanning Tree Protocol (STP) and Link Layer Discovery Protocol (LLDP) control packets, and drop these packets, causing network instability.
  The workaround is to configure port security to shut down the port when a violation occurs.

- **CSCtb62629** (Catalyst Switches 3750 and 3560)
  A Catalyst 3750V2 or Catalyst 3560V2 switch does not supply inline power to PoE devices when the switch is cold-booted from RPS DC power, that is after you disconnect all power to the switch and then reconnect RPS power.
  This problem is seen only on Catalyst 3560V2 or 3750V2 switches, not on non-V2 switches.
  The workaround is to configure a soft reload of the switch by entering the **reload** privileged EXEC command. This causes the inline power to work, even when the RPS is the only source of power.

- **CSCtc57809**
  Switches running Cisco IOS Release 12.2(52)SE might reload after you enter the **no mac address-table static mac-address vlan vlan-id interface interface-id** global configuration command if the interface is up and the MAC address was dynamically learned before it was changed to static.
  Use one of these workarounds:
  - Clear the dynamic MAC address table when configuring static MAC addresses as in this example:
    ```
    Switch(config)# no mac address-table learning vlan vlan_id
    Switch(config)# clear mac-address-table dynamic mac_address
    Switch(config)# mac address-table static mac_address vlan vlan_id interface interface_id
    Switch(config)# mac address-table learning vlan vlan_id
    ```
  - Downgrade to Cisco IOS Release 12.2(50)SE.
  - Upgrade to Cisco IOS Release 12.2(53)SE if available.
- CSCtc77969 (Catalyst Switches 3750, 2975, and 2960-S)
  When PAgP or LACP EtherChannels are configured on a switch stack and the stack reloads, entering a `show interface` or `show etherchannel` summary privileged EXEC command when the stack comes up can cause the console to lock up.
  There is no workaround.

- CSCtd29049
  A switch that has at least one trunk port configured might fail when you configure more than 950 VLANs by using the `vlan vlan-id` global configuration command.
  There is no workaround.

- CSCtd81955
  When you configure more than one EnergyWise domain in a Layer 2 broadcast domain, IP connectivity to the switch might be lost, high CPU usage might occur on the switch, and a broadcast storm might occur in the subnet.
  The workaround is to configure only a single EnergyWise domain in the Layer 2 broadcast domain.

- CSCte00827 (Catalyst Switches 3750, 3560, 2960-S, and 2960)
  When a port that is configured for Switched Port Analyzer (SPAN) goes up and down, a memory leak occurs in the ‘hpm main’ process.
  There is no workaround.

- CSCte14603
  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.
  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:
  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- CSCte94620
  After you apply an ACL, these messages appear:
  `%IPACCESS-4-INVALIDACL: Invalid ACL field: Acl number is 0`
  `%IPACCESS-4-INVALIDACL: Invalid ACL field: Acl type is 145`
  There is no workaround.

- CSCtf19991
If the RADIUS authentication server is unavailable and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the connected port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. After the server is available, the client is not reinitialized and moved out of the critical VLAN.

There is no workaround.

- CSCf33948
  A PC in 802.1x or multidomain authentication (MDA) mode is connected to an IP phone and connected to a MDA-enabled switch port. After the PC and phone are authenticated on the port, the PC is down. The port does not automatically reauthenticate the PC.
  There is no workaround.

- CSCf59354 (Cisco EtherSwitch service modules)
  When a device is connected to a Fast Ethernet port, it can flap.
  The workaround is to use the `power inline never` interface configuration command to disable power to the port.

- CSCfg78276 (Catalyst Switches 3750, 3560, 2960-S, and 2960)
  A switch running Cisco IOS Release 12.2(53)SE1 stops when IEEE 802.1x authentication is enabled.
  The workaround is to apply a VLAN that the RADIUS server assigned to the switch.

- CSCf26941 (Catalyst Switches 3750, 3560, 2960-S, and 2960)
  Multidomain authentication (MDA) with guest VLAN or MAC authentication bypass (MAB) as a fallback method is enabled on a switch running Cisco IOS Release 12.2(53)SE. When a non-802.1x client is connected to a IP phone and the phone connected to a switch port shuts down and then restarts, the client MAC address status is drop in the MAC address table. It takes 5 minutes for the client to access the network.
  The workaround is to use another software release, such as Cisco IOS Release 12.2(44)SE2.

- CSCfg41473 (Catalyst Switch 3750)
  A memory shortage occurs when transceiver module diagnostic tests run. For example, this occurs when you enter the `show interface transceiver detail` privileged command or when SNMP or a network management system (NMS), such as Cisco Network Assistance or Cisco Works, uses the command.
  The workaround is to restart the switch.

- CSCfg47738
  This error message is displayed after copying a configuration file to the running configuration file fails:
  ```
  %Error opening system:/running-config (No such file or directory)
  ```
  The output of the `dir system:/` EXEC command also does not show a running configuration file.
  The workaround is to reload the switch.

- CSCfg18118 (Catalyst Switches 3750, 2975, and 2960-S)
  When VTP pruning is enabled in a VTP domain, the switch in VTP server mode sends advertisements to neighboring switches. If the VTP and VLAN configuration for neighboring ports is not updated, VLANs on those ports can be pruned, causing a network traffic outage.
  The workaround is to disable VTP pruning.

- CSCf67625 (Catalyst Switch 3750V2)
After you upgrade the software on a Catalyst 3750V2 switch to Cisco IOS Release 12.2(53)SE2, the stack ports flap or are down.
The workaround is to use Cisco IOS Release 12.2(52)SE or earlier.

- **CSCti04980**
  After you upgrade the switch software to Cisco IOS Release 12.2(55)SE, enhanced auto-QoS commands are generated when
  - auto-QoS is enabled on an interface
  and
  - **mls qos** command is not enabled on the switch
If the **mls qos** command was already enabled on the switch, enhanced auto-QoS commands are generated only when you configure one of these commands:
  - **auto qos classify** [police]
  - **auto qos trust** {cos | dscp}
  - **auto qos video** {cts | ip-camera}
Cisco IOS Release 12.2(55)SE supports implicit and explicit migration to enhanced auto-QoS configurations.
  - Implicit migration to enhanced auto-QoS occurs on a switch running legacy auto-QoS when you configure the **auto qos video**, **auto qos trust**, or **auto qos classify** command on an interface. Global and interface configurations on the switch migrate to the enhanced video or trust auto-QoS configurations.
  - Explicit migration to enhanced auto-QoS occurs on a switch when you enable the **auto qos srnd4** global configuration command. You can configure the [no] form of this command after you remove auto-QoS functionality from all switch interfaces.

- **CSCuw49951**
The command **ip tcp adjust-mss** is not supported on the switch.
  There is no workaround.
Documentation Updates

- Control Plane Protection, page 66
- Updates to the Software Configuration Guide, page 66
- Updates to the Catalyst 2960 and 2960-S and Catalyst 2975 Software Configuration Guides and Command References, page 67
- Updates to the System Message Guides, page 70
- Updates to the Catalyst 3750 and 3560, and 2960 Hardware Installation Guide, page 79
- Updates for the Catalyst 2960 Switch Hardware Installation Guide, page 80
- Update to the Getting Started Guide, page 81
- Update to the Regulatory Compliance and Safety Information for the Catalyst 2960 Switch, page 81
- Update to the Catalyst 3750, 3560, 2975, and 2960 Switch Command Reference, page 83

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 as logging or forwarding of packets.

Updates to the Software Configuration Guide

In the “Configuring RIP for IPv6” section in the “Configuring IPv6 Unicast Routing” chapter, the task table is incorrect. This is the correct table:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 ipv6 router rip name</td>
<td>Configure an IPv6 RIP routing process, and enter router configuration mode for the process.</td>
</tr>
<tr>
<td>Step 3 maximum-paths number-paths</td>
<td>(Optional) Define the maximum number of equal-cost routes that IPv6 RIP can support. The range is from 1 to 32, and the default is 16 routes.</td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 5 interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 interface to configure.</td>
</tr>
<tr>
<td>Step 6 ipv6 rip name enable</td>
<td>Enable the specified IPv6 RIP routing process on the interface.</td>
</tr>
</tbody>
</table>
Documentation Updates

Updates to the Catalyst 2960 and 2960-S and Catalyst 2975 Software Configuration Guides and Command References

In the “Configuring SDM Templates” chapter and for the `sdm prefer` global configuration command and the `show sdm prefer` privileged EXEC command, the LAN base routing template has incorrect values. The corrected values are:

- number of IPv4 unicast routes: 4.25K should be: 0.75K
- number of directly-connected IPv4 hosts: 4K should be: 0.75K
- number of indirect IPv4 routes: 0.256 should be 16

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

Configuring Critical Voice VLAN

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

For data traffic, you can configure inaccessible authentication bypass, or critical authentication, to allow traffic to pass through on the native VLAN when the server is not available. If the RADIUS authentication server is unavailable (down) and inaccessible authentication bypass is enabled, the switch grants the client access to the network and puts the port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. When the switch cannot reach the configured RADIUS servers and new hosts cannot be authenticated, the switch connects those hosts to critical ports. A new host trying to connect to the critical port is moved to a user-specified access VLAN, the critical VLAN, and granted limited authentication.
With this release, you can enter the `authentication event server dead action authorize voice` interface configuration command to configure the critical voice VLAN feature. When the ACS does not respond, the port goes into critical authentication mode. When traffic coming from the host is tagged with the voice VLAN, the connected device (the phone) is put in the configured voice VLAN for the port. The IP phones learn the voice VLAN identification through CDP (Cisco devices) or through LLDP or DHCP.

**Note**

Critical Voice VLAN is supported on Cisco IOS Release 12.2(55)SE5 and higher.

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

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 radius-server dead-criteria time time tries tries</td>
<td>Sets the conditions that are used to decide when a RADIUS server is considered unavailable or down (dead).</td>
</tr>
<tr>
<td></td>
<td>• The range for <code>time</code> is from 1 to 120 seconds. The switch dynamically determines a default <code>seconds</code> value between 10 and 60 seconds.</td>
</tr>
<tr>
<td></td>
<td>• The range for <code>tries</code> is from 1 to 100. The switch dynamically determines a default <code>tries</code> parameter between 10 and 100.</td>
</tr>
<tr>
<td>Step 3 radius-server deadtime minutes</td>
<td>(Optional) Sets the number of minutes during which a RADIUS server is not sent requests. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.</td>
</tr>
</tbody>
</table>
Step 4

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| radius-server host ip-address [acct-port udp-port] [auth-port udp-port] [test username name [idle-time time] [ignore-acct-port] [ignore-auth-port]] [key string] | Configures the RADIUS server parameters:  
  - **acct-port udp-port**—Specifies the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646.  
  - **auth-port udp-port**—Specifies the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645.  
  
  **Note** You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values.  
  - **test username name**—Enables automatic testing of the RADIUS server status, and specifies the username to be used.  
  - **idle-time time**—Sets the interval of time in minutes after which the switch sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour).  
  - **ignore-acct-port**—Disables testing on the RADIUS-server accounting port.  
  - **ignore-auth-port**—Disables testing on the RADIUS-server authentication port.  
  - For **key string**, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.  
  
  **Note** Always configure the key as the last item in the radius-server host command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon.  
  You can also configure the authentication and encryption key by using the radius-server key {0 string | 7 string | string} global configuration command. |

Step 5

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface-id</td>
<td>Specifies the port to be configured and enters interface configuration mode.</td>
</tr>
</tbody>
</table>

Step 6

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| authentication event server dead action {authorize | reinitialize} vlan vlan-id | Configures a critical VLAN to move hosts on the port if the RADIUS server is unreachable:  
  - **authorize**—Moves any new hosts trying to authenticate to the user-specified critical VLAN.  
  - **reinitialize**—Moves all authorized hosts on the port to the user-specified critical VLAN. |

Step 7

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchport voice vlan vlan-id</td>
<td>Specifies the voice VLAN for the port. The voice VLAN cannot be the same as the critical data VLAN configured in Step 6.</td>
</tr>
</tbody>
</table>

Step 8

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication event server dead action authorize voice</td>
<td>Configures critical voice VLAN to move data traffic on the port to the voice VLAN if the RADIUS server is unreachable.</td>
</tr>
</tbody>
</table>

Step 9

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Step 10

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show authentication interface interface-id</td>
<td>(Optional) Verifies your entries.</td>
</tr>
</tbody>
</table>

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

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

Updates to the System Message Guides

New System Messages

Error Message AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface [chars], new MAC address ([enet]) is seen. AuditSessionID [chars]

Explanation A host on the interface attempted to gain access to the network or attempted an authentication. The interface mode does not support the number of hosts that are attached to the interface. This is a security violation, and the interface has been error-disabled. The first [chars] is the interface, [enet] is the Ethernet address of the host, and the second [chars] is the session ID.

Recommended Action Make sure that the interface is configured to support the number of hosts that are attached to it. Enter the shutdown interface configuration command followed by no shutdown interface configuration command to restart the interface.

Error Message AUTHMGR-5-VLANASSIGN: VLAN [dec] assigned to Interface [chars]
AuditSessionID [chars]

Explanation A VLAN was assigned. [dec] is the VLAN ID, the first [chars] is the interface, and the second [chars] is the session ID.

Recommended Action No action is required.

Error Message AUTHMGR-7-FAILOVER: Failing over from [chars] for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation The authorization manager is failing over from the current authentication method to another method. The first [chars] is the current authentication method, the second [chars] is the client ID, the third [chars] is the interface, and the fourth [chars] is the session ID.

Recommended Action No action is required.
Error Message  AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client (chars) on Interface [chars] AuditSessionID [chars]

Explanation  All available authentication methods have been tried for the client, but authentication has failed. 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. If local authorization has been configured, the port will be authorized based on the local authorization method. Otherwise, authentication will restart according to the configured reauthentication period.


Explanation  The results of the authentication. The first [chars] is the status of the authentication, the second [chars] is the authentication method, the third [chars] is the client ID, the fourth [chars] is the interface, and the fifth [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-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-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.

**Error Message** EPM-6-AUTH_ACL: POLICY [chars] | EVENT [chars]

**Explanation** The switch has sent or received a download request for a downloadable ACL (dACL). The first [chars] is the dACL policy. The second [chars] is the event.

**Recommended Action** No action is required.

**Error Message** HARDWARE-1-TCAM_ERROR: [traceback] Found error in [chars] TCAM Space and not able to recover the error

**Note** This message is not applicable on Catalyst 2960-S switches.

**Explanation** The switch cannot fix a ternary content addressable memory (TCAM) integrity error. [chars] is memory location with the error: Unassigned TCAM Space, HFTM TCAM Space (the ASIC forwarding TCAM manager space), or HQATM TCAM Space (the TCAM ASIC quality of service [QoS] and access control list [ACL] TCAM manager space).

**Recommended Action** Restart the switch.

**Error Message** HARDWARE-3-ASICNUM_ERROR: [traceback] Port-ASIC number [dec] is invalid

**Explanation** The port ASIC number is invalid. [dec] is the port ASIC number.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message** HARDWARE-3-PORTNUM_ERROR: [traceback] port number [dec] is invalid

**Explanation** The port number is out of range. [dec] is the port number.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.
Error Message  HULC_LICENSE-1-LICENSE_REGISTER_FAILED: [chars] - rc = [dec]

Note  This message applies only to Catalyst 2960-S switches.

Explanation  The licensing initialization failed. [chars] explains what part of the license registration failed, and [dec] is the type of license initialization error.

Recommended Action  Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message  IFMGR-3-IFINDEX_PERSIST_ENTRY_CORRUPT: [chars] seems to be corrupted. Trying to read [dec] size

Explanation  The ifIndex table is corrupted. [chars] is the path to the IfIndex file, and [dec] is the number of bytes that was being read from the ifIndex table when the corruption was detected.

Recommended Action  Delete the ifindex table.

Error Message  IFMGR-3-INVALID_PERSISTENT_DATA: Invalid persistent data

Explanation  The interface manager attempts to write invalid persistent data.

Recommended Action  Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message  ILET-1-AUTHENTICATION_FAIL: This Switch may not have been manufactured by Cisco or with Cisco’s authorization. This product may contain software that was copied in violation of Cisco’s license terms. If your use of this product is the cause of a support issue, Cisco may deny operation of the product, support under your warranty or under a Cisco technical support program such as Smartnet. Please contact Cisco’s Technical Assistance Center for more information.

Explanation  A license authentication failure occurred for the switch.

Recommended Action  Contact your Cisco sales representative for assistance.

Error Message  ILET-1-DEVICE_AUTHENTICATION_FAIL: The [chars] inserted in this switch may not have been manufactured by Cisco or with Cisco’s authorization. If your use of this product is the cause of a support issue, Cisco may deny operation of the
product, support under your warranty or under a Cisco technical support program such as Smartnet. Please contact Cisco's Technical Assistance Center for more information.

**Explanation**  A license authentication failure occurred for a component that was inserted in the switch. [chars] is the component.

**Recommended Action**  Contact your Cisco sales representative for assistance.

**Error Message**  PLATFORM-6-FLEXSTACK_INSERTED: FlexStack module inserted [chars]

**Note**  This message applies only to Catalyst 2960-S switches.

**Explanation**  The switch has detected a FlexStack module. [chars] is the slot.

**Recommended Action**  No action is required.

**Error Message**  PLATFORM-6-FLEXSTACK_REMOVED: FlexStack module removed [chars]

**Note**  This message applies only to Catalyst 2960-S switches.

**Explanation**  The switch has detected that a FlexStack module has been removed. [chars] is the slot.

**Recommended Action**  No action is required.

**Error Message**  POWERNET_ISSU-4-SM_EW_DOMAIN_MISMATCH: Energywise domain of EtherSwitch is [chars], recommended to have [chars].

**Note**  This message applies only to Cisco EtherSwitch service modules.

**Explanation**  The EnergyWise domain of the service module does not match that of the switch. The first [chars] is the EnergyWise domain of the service module. The second [chars] is the EnergyWise domain of the router.

**Recommended Action**  Configure the EnergyWise domain of the service module to match that of the switch. If the message recurs, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.
Error Message  SCHED-3-UNEXPECTEDEVENT: [traceback] [process information] Process received unknown event (maj [hex], min [hex])

Explanation  A process did not handle an event. The first [hex] is the major event number, and the second [hex] is the minor event number, both of which allow you to identify the event that occurred.

Recommended Action  Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Modified System Messages

Error Message  DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation  The authentication result was overridden. 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_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 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 message 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 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 port mode so that it is no longer a PVLAN host port, or use a valid secondary VLAN.

Note  This message applies to switches running the IP base image.
Error Message DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN \( \text{[dec]} \), whose primary VLAN does not exist or is shutdown, to 802.1x port \( \text{[chars]} \) AuditSessionID \( \text{[chars]} \)

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

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

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

Error Message DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN \( \text{[dec]} \) to non-PVLAN host 802.1x port \( \text{[chars]} \) AuditSessionID \( \text{[chars]} \)

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. \( \text{[dec]} \) is the VLAN, the first \( \text{[chars]} \) is the port, and the second \( \text{[chars]} \) is the session ID.

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

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

Error Message DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN \( \text{[dec]} \) to 802.1x port \( \text{[chars]} \), which is configured as a SPAN destination AuditSessionID \( \text{[chars]} \)

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

Explanation Multi-Domain Authentication (MDA) host mode cannot start when the configured data VLAN on a port is the same as the voice VLAN. \( \text{[chars]} \) 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 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 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 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.

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] AuditSessionID [chars]

Explanation  An attempt was made to assign an invalid VLAN to an 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 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 shut down, or use another VLAN.

Error Message  DOT1X_SWITCH-5-ERR_VLAN_ON_ROUTED_PORT: Attempt to assign VLAN [dec] to routed 802.1x port [chars] AuditSessionID [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, the first [chars] is the port, and the second [chars] is the session ID.

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] AuditSessionID [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, the first [chars] is the port, and the second [chars] is the session ID.

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] AuditSessionID [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, the first [chars] is the port, and the second [chars] is the session ID.

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 AuditSessionID [chars]

Explanation  Remote SPAN should not be enabled on a VLAN with IEEE 802.1x-enabled. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

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

Error Message  SPANTREE-2-BLOCK_BPDUGUARD_VP: Received BPDU on port [chars], vlan [dec] with BPDU Guard enabled. Disabling vlan.

Explanation  A BPDU was received on the interface and the VLAN specified in the error message. The spanning tree BPDU guard feature was enabled and configured to shut down the VLAN. As a result, the VLAN was placed in the error-disabled state. [chars] is the interface, and [dec] is the VLAN.

Recommended Action  Either remove the device sending BPDUs, or disable the BPDU guard feature. The BPDU guard feature can be locally configured on the interface or globally configured on all ports that have Port Fast enabled. Re-enable the interface and vlan by entering the clear errdisable privileged EXEC command.
Deleted System Messages

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

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

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

Error Message SW_VLAN-4-VTP_USER_NOTIFICATION: VTP protocol user notification: [chars].

Updates to the Catalyst 3750 and 3560, and 2960 Hardware Installation Guide

Cisco Ethernet Switches are equipped with cooling mechanisms, such as fans and blowers. However, these fans and blowers can draw dust and other particles, causing contaminant buildup inside the chassis, which can result in a system malfunction.

You must install this equipment in an environment as free as possible from dust and foreign conductive material (such as metal flakes from construction activities).

These standards provide guidelines for acceptable working environments and acceptable levels of suspended particulate matter:

- Network Equipment Building Systems (NEBS) GR-63-CORE
- National Electrical Manufacturers Association (NEMA) Type 1
- International Electrotechnical Commission (IEC) IP-20

This applies to all Cisco Ethernet switches except for these compact models:

- Catalyst 3560-8PC switch—8 10/100 PoE ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)
- Catalyst 2960-8TC switch—8 10/100BASE-T Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)
- Catalyst 2960G-8TC switch—7 10/100/100BASE-T Ethernet ports and 1 dual-purpose port (one 10/100/1000BASE-T copper port and one SFP module slot)
Updates for the **Catalyst 2960 Switch Hardware Installation Guide**

This update is for the “Overview” chapter. These PoE switches were added:

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Supported Software Image</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 2960-48PST-S</td>
<td>LAN-Lite</td>
<td>48 10/100 PoE ports, 2 10/100/1000 ports, and 2 SFP module slots</td>
</tr>
<tr>
<td>Catalyst 2960-24PC-S</td>
<td>LAN-Lite</td>
<td>24 10/100 PoE ports and 2 dual-purpose ports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2 10/100/1000BASE-T copper ports and 2 SFP module slots)</td>
</tr>
<tr>
<td>Catalyst 2960-24LC-S</td>
<td>LAN-Lite</td>
<td>24 10/100 ports (8 of which are PoE) and 2 dual-purpose ports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2 10/100/1000BASE-T copper ports and 2 SFP module slots)</td>
</tr>
</tbody>
</table>

---

**Note**

The PoE sections in the hardware guide also apply to these switches, even though they are not listed in the hardware guide.

This update is for the “Technical Specifications” chapter.

<table>
<thead>
<tr>
<th><strong>Table 9  Catalyst 2960-48PST-S, Catalyst 2960-24PC-S, and Catalyst 2960-24LC-S Specifications</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Requirements</strong></td>
</tr>
<tr>
<td>AC input voltage</td>
</tr>
<tr>
<td>100 to 240 VAC (autoring) 8 to 4 A, 50 to 60 Hz (Catalyst 2960-24PC-S)</td>
</tr>
<tr>
<td>3 to 1.5 A, 50 to 60 Hz (Catalyst 2960-24LC-S)</td>
</tr>
<tr>
<td>5 to 2 A, 50 to 60 Hz (Catalyst 2960-48PST-S)</td>
</tr>
<tr>
<td>DC input voltage for RPS 2300</td>
</tr>
<tr>
<td>+ 12 V ==@ 11.25 A, –48 V ==@ 7.8 A (Catalyst 2960-24PC-S)</td>
</tr>
<tr>
<td>+ 12 V ==@ 8.3 A, –48 V ==@ 2.7 A (Catalyst 2960-24LC-S)</td>
</tr>
<tr>
<td>+12 V ==@ 4 A, –48 V ==@ 7.8 A (Catalyst 2960-48PST-S)</td>
</tr>
<tr>
<td>Power consumption1</td>
</tr>
<tr>
<td>100 W, 341 BTUs per hour (Catalyst 2960-24PC-S)</td>
</tr>
<tr>
<td>51 W, 174 BTUs per hour (Catalyst 2960-24LC-S)</td>
</tr>
<tr>
<td>483 W, 1647 BTUs per hour (Catalyst 2960-48PST-S)</td>
</tr>
<tr>
<td>Power rating</td>
</tr>
<tr>
<td>0.470 KVA (Catalyst 2960-24PC-S)</td>
</tr>
<tr>
<td>0.175 KVA (Catalyst 2960-24LC-S)</td>
</tr>
<tr>
<td>0.5 KVA (Catalyst 2960-48PST-S)</td>
</tr>
<tr>
<td><strong>Power over Ethernet</strong></td>
</tr>
<tr>
<td>15.4 W-per-port maximum, 370-W switch maximum (Catalyst 2960-48PST-S and 24PC-S)</td>
</tr>
<tr>
<td>15.4 W-per-port maximum, 124-W switch maximum (Catalyst 2960-24LC-S).</td>
</tr>
<tr>
<td><strong>Physical Dimensions</strong></td>
</tr>
<tr>
<td>Weight</td>
</tr>
<tr>
<td>12 lb (5.44 kg) (Catalyst 2960-24PC-S)</td>
</tr>
<tr>
<td>10 lb (4.54 kg) (Catalyst 2960-24LC-S)</td>
</tr>
<tr>
<td>12 lb (5.44 kg) (Catalyst 2960-48PST-S)</td>
</tr>
<tr>
<td>Dimensions (H x W x D)</td>
</tr>
<tr>
<td>1.73 x 13 x 17.5 in. (4.39 x 33.02 x 44.45 cm)</td>
</tr>
</tbody>
</table>

1. The power consumption values are for the switch input power.
Update to the Getting Started Guide

When you launch Express Setup, you are prompted for the switch password. Enter the default password, `cisco`. The switch ignores text in the username field. Before you complete and exit Express Setup, you must change the password from the default password, `cisco`.

Update to the Regulatory Compliance and Safety Information for the Catalyst 2960 Switch

This warning applies to the Catalyst 2960 24- and 48-port switches:

Statement 266—Switch Installation Warning

<table>
<thead>
<tr>
<th>Warning</th>
<th>To comply with safety regulations, mount switches on a wall with the front panel facing up. Statement 266</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waarschuwing</td>
<td>Om te voldoen aan de veiligheidsvoorschriften dient u de schakelaars op een muur te monteren met het voorpaneel omhoog. Statement 266</td>
</tr>
<tr>
<td>Veroittus</td>
<td>Turvallisuusmääräykset edellyttävät edellyttävät, että kytkimet kiinnitetään seinäät etupaneeli ylöspäin. Statement 266</td>
</tr>
<tr>
<td>Attention</td>
<td>Pour satisfaire aux dispositions de sécurité, installez les commutateurs muraux avec le panneau frontal vers le haut. Statement 266</td>
</tr>
<tr>
<td>Warnung</td>
<td>Zur Einhaltung der Sicherheitsvorschriften die Schalter so an einer Wand montieren, dass die Frontplatte nach oben zeigt. Statement 266</td>
</tr>
<tr>
<td>Avvertenza</td>
<td>In conformità ai regolamenti di sicurezza, installare i dispositivi switch a muro con il pannello frontale rivolto in su. Statement 266</td>
</tr>
<tr>
<td>Advarsel</td>
<td>For å etterkomme sikkerhetsreglene skal brytere monteres på en vegg med frontpanelet vendt opp. Statement 266</td>
</tr>
<tr>
<td>Aviso</td>
<td>Para cumprir com os regulamentos de segurança, faça a montagem de switches em uma parede com o painel frontal virado para cima. Statement 266</td>
</tr>
<tr>
<td>¡Advertencia!</td>
<td>Para cumplir con las reglas de seguridad, instale los interruptores en una pared con el panel del frente hacia arriba. Statement 266</td>
</tr>
<tr>
<td>Warning!</td>
<td>För att uppfylla säkerhetsföreskrifter skall switcharna monteras på en vägg med frampanelen riktad uppåt. Statement 266</td>
</tr>
</tbody>
</table>

A biztonsági előírások betartása érdekében a kapcsolókat úgy szerelje a falra, hogy az előlapjuk felfelé nézzen.
Предупреждение  В соответствии с положениями безопасности установите переключатели на стене передней панелью наружу.

警告  ектростатическим разрядом. Не дотрагивайтесь до задней панели предметом, поскольку это может привести к поражению

安全既定に準拠するために、フロントパネルを上向きにしてスイッチを壁にマウントします。
auto qos video

Use the `auto qos video` interface configuration command on the switch stack or on a standalone switch to automatically configure quality of service (QoS) for video within a QoS domain. Use the `no` form of this command to return to the default setting.

```
auto qos video {cts | ip-camera}
```

```
no auto qos video {cts | ip-camera}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cts</code></td>
<td>Identify this port as connected to a Cisco TelePresence System and automatically configure QoS for video.</td>
</tr>
<tr>
<td><code>ip-camera</code></td>
<td>Identify this port as connected to a Cisco IP camera and automatically configure QoS for video.</td>
</tr>
</tbody>
</table>

**Defaults**

Auto-QoS video is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

**Table 1-10 Traffic Types, Packet Labels, and Queues**

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>DSCP</th>
<th>VOIP Data Traffic</th>
<th>VOIP Control Traffic</th>
<th>Routing Protocol Traffic</th>
<th>STP1 BPDU2 Traffic</th>
<th>Real-Time Video Traffic</th>
<th>All Other Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>VOIP Data Traffic</td>
<td>46</td>
<td>24, 26</td>
<td></td>
<td>48</td>
<td>56</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>VOIP Control Traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routing Protocol Traffic</td>
<td>48</td>
<td>24, 26</td>
<td></td>
<td>48</td>
<td>56</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>STP1 BPDU2 Traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-Time Video Traffic</td>
<td>34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Other Traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. STP = Spanning Tree Protocol
2. BPDU = bridge protocol data unit
3. DSCP = Differentiated Services Code Point
4. CoS = class of service

**Table 1-11 Auto-QoS Configuration for the Ingress Queues**

<table>
<thead>
<tr>
<th>Ingress Queue</th>
<th>Queue Number</th>
<th>CoS-to-Queue Map</th>
<th>Queue Weight (Bandwidth)</th>
<th>Queue (Buffer) Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRR1 shared</td>
<td>1</td>
<td>0, 1, 2, 3, 6, 7</td>
<td>70 percent</td>
<td>90 percent</td>
</tr>
<tr>
<td>Priority</td>
<td>2</td>
<td>4, 5</td>
<td>30 percent</td>
<td>10 percent</td>
</tr>
</tbody>
</table>

1. SRR = shaped round robin. Ingress queues support shared mode only.
Use this command to configure QoS appropriate for video traffic within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-Qos configures the switch for video connectivity with a Cisco TelePresence system and a Cisco IP camera.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration after you enable auto-QoS.

Note
The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (mls qos global configuration command), and other global configuration commands are added.
- After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes AutoQoS in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

<table>
<thead>
<tr>
<th>Egress Queue</th>
<th>Queue Number</th>
<th>CoS-to-Queue Map</th>
<th>Queue Weight (Bandwidth)</th>
<th>Queue (Buffer) Size for Gigabit-Capable Ports</th>
<th>Queue (Buffer) Size for 10/100 Ethernet Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority (shaped)</td>
<td>1</td>
<td>4, 5</td>
<td>up to 100 percent</td>
<td>25 percent</td>
<td>15 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>2</td>
<td>2, 3, 6, 7</td>
<td>10 percent</td>
<td>25 percent</td>
<td>25 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>3</td>
<td>0</td>
<td>60 percent</td>
<td>25 percent</td>
<td>40 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>4</td>
<td>1</td>
<td>20 percent</td>
<td>25 percent</td>
<td>20 percent</td>
</tr>
</tbody>
</table>

Command Modes
Interface configuration

Command History
Release   Modification
12.2(55)SE This command was introduced.

Usage Guidelines

<table>
<thead>
<tr>
<th>Table 1-12 Auto-QoS Configuration for the Egress Queues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Queue</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Priority (shaped)</td>
</tr>
<tr>
<td>SRR shared</td>
</tr>
<tr>
<td>SRR shared</td>
</tr>
<tr>
<td>SRR shared</td>
</tr>
</tbody>
</table>
To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the `debug auto qos` privileged EXEC command to enable auto-QoS debugging. For more information, see the `debug auto qos` command.

To disable auto-QoS on a port, use the `no auto qos video` interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the `no auto qos video` command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the `no mls qos` global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

### Examples

This example shows how to enable auto-QoS for a Cisco Telepresence interface with conditional trust. The interface is trusted only if a Cisco Telepresence device is detected; otherwise, the port is untrusted.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos video cts
```

You can verify your settings by entering the `show auto qos video interface interface-id` privileged EXEC command.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug auto qos</code></td>
<td>Enables debugging of the auto-QoS feature.</td>
</tr>
<tr>
<td><code>mls qos trust</code></td>
<td>Configures the port trust state.</td>
</tr>
<tr>
<td><code>srr-queue bandwidth share</code></td>
<td>Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.</td>
</tr>
<tr>
<td><code>queue-set</code></td>
<td>Maps a port to a queue-set.</td>
</tr>
<tr>
<td><code>show auto qos</code></td>
<td>Displays auto-QoS information.</td>
</tr>
<tr>
<td><code>show mls qos interface</code></td>
<td>Displays QoS information at the port level.</td>
</tr>
</tbody>
</table>

### Related Documentation

These documents provide complete information about the Catalyst 3750, 3560, 2975, 2960-S and 2960 switches and the Cisco EtherSwitch service modules and are available at Cisco.com:

These documents provide complete information about the Catalyst 3750 switches and the Cisco EtherSwitch service modules:

- Catalyst 3750 Switch Software Configuration Guide
- Catalyst 3750 Switch Command Reference
- Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide
- Catalyst 3750 Switch Hardware Installation Guide
- Catalyst 3750 Getting Started Guide
- Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide
- Regulatory Compliance and Safety Information for the Catalyst 3750 Switch

These documents provide complete information about the Catalyst 3750G Integrated Wireless LAN Controller Switch and the integrated wireless LAN controller and are available at cisco.com:

- Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide
- Release Notes for Cisco Wireless LAN Controller and Lightweight Access Point, Release 4.0.x.0
- Cisco Wireless LAN Controller Configuration Guide, Release 4.0
- Cisco Wireless LAN Controller Command Reference, Release 4.0

These documents provide complete information about the Catalyst 3560 switches:

- Catalyst 3560 Switch Software Configuration Guide
- Catalyst 3560 Switch Command Reference
- Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide
- Catalyst 3560 Switch Hardware Installation Guide
- Catalyst 3560 Switch Getting Started Guide
- Regulatory Compliance and Safety Information for the Catalyst 3560 Switch

These documents provide complete information about the Catalyst 2975 switches:

- Catalyst 2975 Switch Software Configuration Guide
- Catalyst 2975 Switch Command Reference
- Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide
- Catalyst 2975 Switch Hardware Installation Guide
- Catalyst 2975 Switch Getting Started Guide
- Regulatory Compliance and Safety Information for the Catalyst 2975 Switch

These documents provide complete information about the Catalyst 2960 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:
• Device manager online help (available on the switch)
• 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
  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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
This document is to be used in conjunction with the documents listed in the “Obtaining Documentation and Submitting a Service Request” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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.

© 2017 Cisco Systems, Inc. All rights reserved.