Release Notes for Catalyst 3750-X, 3750-E, 3560-X, and 3560-E Switches, Cisco IOS Release 15.0(2)SE and Later

November 29, 2019

Cisco IOS Release 15.0(2)SE and higher runs on Catalyst 3750-X, Catalyst 3750-E, Catalyst 3560-X, and Catalyst 3560-E switches and on Cisco enhanced EtherSwitch service modules.

The Catalyst 3750-X and 3750-E switches support stacking through Cisco StackWise Plus technology. The Catalyst 3750-X also supports StackPower. The Catalyst 3560-X switches, Catalyst 3560-E switches, and the Cisco enhanced EtherSwitch service modules do not support switch stacking.

Unless otherwise noted, the term switch refers to a standalone switch and to a switch stack. Cisco enhanced EtherSwitch service modules and Catalyst 3560-E switches support the same features.

For more information, see the Deciding Which Files to Use, page 11 and the “Related Documentation” section on page 72.

These release notes include important information about Cisco IOS release 15.0(2)SE and higher, and later and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the show version privileged EXEC command. See the “Finding the Software Version and Feature Set” section on page 10.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “Deciding Which Files to Use” section on page 11.

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

- “System Requirements” section on page 2
- “Upgrading the Switch Software” section on page 10
- “Installation Notes” section on page 15
- “New Software Features” section on page 15
- “Limitations and Restrictions” section on page 22
- “Important Notes” section on page 35
- “Cisco Bug Search Tool” section on page 37
- “Open Caveats” section on page 37
- “Resolved Caveats” section on page 40
- “Related Documentation” section on page 72
- “Obtaining Documentation and Submitting a Service Request” section on page 74

System Requirements

- “Supported Hardware” section on page 2
- “Device Manager System Requirements” section on page 9
- “Cluster Compatibility” section on page 10
- “CNA Compatibility” section on page 10

Supported Hardware

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

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3560X-24T-E</td>
<td>24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560X-48T-E</td>
<td>48 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560X-24P-E</td>
<td>24 10/100/1000 PoE+ 2 ports, 1 network module slot, 715 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560X-48P-E</td>
<td>48 10/100/1000 PoE+ 2 ports, 1 network module slot, 715 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560X-48PF-E</td>
<td>48 10/100/1000 PoE+ 2 ports, 1 network module slot, 1100 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750X-24T-E</td>
<td>24 10/100/1000 Ethernet ports, StackWise Plus, StackPower, 1 network module slot, 350 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
</tbody>
</table>
### Table 1  Catalyst 3750-X and Catalyst 3560-X Supported Hardware (continued)

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3750X-48T-E</td>
<td>48 10/100/1000 Ethernet ports, StackWise Plus, StackPower, 1 network module slot, 350 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750X-24P-E</td>
<td>24 10/100/1000 PoE+² ports, StackWise Plus, StackPower, 1 network module slot, 715 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750X-48P-E</td>
<td>48 10/100/1000 PoE+² ports, StackWise Plus, StackPower, 1 network module slot, 715 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750X-48PF-E</td>
<td>48 10/100/1000 PoE+² ports, StackWise Plus, StackPower, 1 network module slot, 1100 W power supply; IP Services feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-12S-S</td>
<td>12 SFP module slots, StackWise Plus, StackPower, 1 network module slot, 350-W power supply; IP Base feature set</td>
<td>12.2(55)SE5</td>
</tr>
<tr>
<td>Catalyst 3750-X-24S-S</td>
<td>24 SFP module slots, StackWise Plus, StackPower, 1 network module slot, 350-W power supply; IP Base feature set</td>
<td>12.2(55)SE5</td>
</tr>
<tr>
<td>Catalyst 3750-X-12S-E</td>
<td>12 SFP module slots, StackWise Plus, StackPower, 1 network module slot, 350-W power supply; IP Services feature set</td>
<td>12.2(55)SE5</td>
</tr>
<tr>
<td>Catalyst 3750-X-24T-L</td>
<td>24 10/100/1000 Ethernet ports, StackWise Plus, 1 network module slot, 350 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-48T-L</td>
<td>48 10/100/1000 Ethernet ports, StackWise Plus, 1 network module slot, 350 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-24P-L</td>
<td>24 10/100/1000 PoE+¹ ports, StackWise Plus, 1 network module slot, 715 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-48P-L</td>
<td>48 10/100/1000 PoE+² ports, StackWise Plus, 1 network module slot, 715 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-48PF-L</td>
<td>48 10/100/1000 PoE+² ports, StackWise Plus, 1 network module slot, 1100 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-24T-S</td>
<td>24 10/100/1000 Ethernet ports, StackWise Plus, StackPower, 1 network module slot, 350 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-48T-S</td>
<td>48 10/100/1000 Ethernet ports, StackWise Plus, StackPower, 1 network module slot, 350 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-24P-S</td>
<td>24 10/100/1000 PoE+² ports, StackWise Plus, StackPower, 1 network module slot, 715 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-48P-S</td>
<td>48 10/100/1000 PoE+² ports, StackWise Plus, StackPower, 1 network module slot, 715 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3750-X-48PF-S</td>
<td>48 10/100/1000 PoE+² ports, StackWise Plus, StackPower, 1 network module slot, 1100 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
</tbody>
</table>
### System Requirements

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

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3560-X-24T-L</td>
<td>24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-48T-L</td>
<td>48 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-24P-L</td>
<td>24 10/100/1000 PoE+² ports, 1 network module slot, 715 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-48P-L</td>
<td>48 10/100/1000 PoE+² ports, 1 network module slot, 715 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-48PF-L</td>
<td>48 10/100/1000 PoE+² ports, 1 network module slot, 1100 W power supply; LAN Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-24T-S</td>
<td>24 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-48T-S</td>
<td>48 10/100/1000 Ethernet ports, 1 network module slot, 350 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-24P-S</td>
<td>24 10/100/1000 PoE+² ports, 1 network module slot, 715 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-48P-S</td>
<td>48 10/100/1000 PoE+² ports, 1 network module slot, 715 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Catalyst 3560-X-48PF-S</td>
<td>48 10/100/1000 PoE+² ports, 1 network module slot, 1100 W power supply; IP Base feature set</td>
<td>12.2(53)SE2</td>
</tr>
</tbody>
</table>
| SFP Modules | 100FX-SFP  
GE SFPLX/LH  
GE SFP SX  
1000BASE-LX/LH  
1000BASE-SX  
1000BASE-ZX  
1000BASE-BX10-D  
1000BASE-BX10-U  
1000BASE-T  
100BASE-FX  
CWDM²  
DWDM³ | 12.2(53)SE2 |

**Note** For a complete list of supported SFP modules, see the hardware installation guide or the data sheets at:  

| SFP+ Modules | SFP-10G-SR  
SFP-10G-LR  
SFP-10G-LRM  
SFP-H10GB CU1M  
SFP-H10GB CU3M  
SFP-H10GB CU5M | 12.2(53)SE2 |
## System Requirements

### SFP+ Modules
- SFP-10G-ER

### Support for these SFP+ modules
- Only version 02 (or later) of the CX1 cables are supported:
  - SFP-H10GB-CU1M
  - SFP-H10GB-CU3M
  - SFP-H10GB-CU5M

### SFP module patch cable
- CAB-SFP-50CM

### Power supply modules
- C3KX-PWR-1100WAC
- C3KX-PWR-715WAC
- C3KX-PWR-350WAC
- C3KX-PWR-440WDC
- C3KX-PSBAY-BLNK

**Note**: For power supply module descriptions and configurations supported on switch models, see the hardware installation guide.

### C3KX-NM-10G
- 10-Gigabit Ethernet Network Module
  - Four SFP slots.
  - Two slots support only 1-Gigabit SFP modules, two slots support either 1-Gigabit SFP or 10-Gigabit SFP+ modules.

### C3KX-NM-1G
- 1-Gigabit Ethernet Network Module
  - Four 1-Gigabit SFP module slots.

### C3KX-NM-10GT
- 10-Gigabit Ethernet Network Module
  - Two 10-Gigabit Ethernet (copper) ports.
  **Note**: To configure the port speed to 1 Gigabit per second, use the `hw-module switch` global configuration command.

### eXpandable power system (XPS)
- Cisco XPS 2200

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP+ Modules</td>
<td>SFP-10G-ER</td>
<td>15.0(2)SE</td>
</tr>
<tr>
<td>Support for these SFP+ modules</td>
<td>Only version 02 (or later) of the CX1 cables are supported:</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td></td>
<td>SFP-H10GB-CU1M</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SFP-H10GB-CU3M</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SFP-H10GB-CU5M</td>
<td></td>
</tr>
<tr>
<td>SFP module patch cable</td>
<td>CAB-SFP-50CM</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Power supply modules</td>
<td>C3KX-PWR-1100WAC</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td></td>
<td>C3KX-PWR-715WAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C3KX-PWR-350WAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C3KX-PWR-440WDC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C3KX-PSBAY-BLNK</td>
<td></td>
</tr>
<tr>
<td>C3KX-NM-10G</td>
<td>Four SFP slots.</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>10-Gigabit Ethernet Network Module</td>
<td>Two slots support only 1-Gigabit SFP modules, two slots support either 1-Gigabit SFP or 10-Gigabit SFP+ modules.</td>
<td></td>
</tr>
<tr>
<td>C3KX-NM-1G</td>
<td>Four 1-Gigabit SFP module slots.</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>C3KX-NM-10GT</td>
<td>Two 10-Gigabit Ethernet (copper) ports.</td>
<td>15.0(1)SE</td>
</tr>
<tr>
<td>10-Gigabit Ethernet Network Module</td>
<td><strong>Note</strong>: To configure the port speed to 1 Gigabit per second, use the <code>hw-module switch</code> global configuration command.</td>
<td></td>
</tr>
<tr>
<td>eXpandable power system (XPS)</td>
<td>Cisco XPS 2200</td>
<td>12.2(55)SE1</td>
</tr>
<tr>
<td>Power supply modules</td>
<td>PWR-C1-350WAC</td>
<td>15.0(2)SE5</td>
</tr>
<tr>
<td></td>
<td>PWR-C1-715WAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PWR-C1-1100WAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PWR-C1-440WDC</td>
<td></td>
</tr>
</tbody>
</table>

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

### Table 2  
Catalyst 3750-E and 3560-E Switches and Cisco Enhanced EtherSwitch Service Module Supported Hardware

<table>
<thead>
<tr>
<th>Switch Hardware</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 3750E-24TD</td>
<td>24 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3750E-48TD</td>
<td>48 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3750E-24PD</td>
<td>24 10/100/1000 PoE(^1) ports, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3750E-48PD</td>
<td>48 10/100/1000 ports with 370 W of PoE, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3750E-48PD Full Power</td>
<td>48 10/100/1000 ports with 740 W of PoE, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560E-24TD</td>
<td>24 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560E-48TD</td>
<td>48 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560E-24PD</td>
<td>24 10/100/1000 PoE ports, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560E-48PD</td>
<td>48 10/100/1000 ports with 370 W of PoE, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560E-48PD Full Power</td>
<td>48 10/100/1000 ports with 740 W of PoE, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560E-12D</td>
<td>12 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(40)EX</td>
</tr>
<tr>
<td>Cisco Catalyst 3560E-12SD</td>
<td>12 SFP(^2) module slots, 2 10-Gigabit Ethernet X2 module slots</td>
<td>Cisco IOS Release 12.2(44)SE</td>
</tr>
<tr>
<td>Cisco X2 transceiver modules</td>
<td>X2-10GB-SR V02 or later X2-10GB-LR V03 or later X2-10GB-ER V02 or later X2-10GB-CX4 V03 or later X2-10GB-LX4 V03 or later X2-10GB-LRM 10 Gigabit Ethernet X2 ZR optical modules</td>
<td>Cisco IOS Release 12.2(35)SE2, Cisco IOS Release 12.2(40)SE, Cisco IOS Release 12.2(50)SE</td>
</tr>
<tr>
<td>Cisco TwinGig Converter Module</td>
<td>Dual SFP X2 converter module to allow the switch to support SFP Gigabit Ethernet modules</td>
<td>Cisco IOS Release 12.2(35)SE2</td>
</tr>
</tbody>
</table>
## System Requirements

### SFP modules

- 1000BASE-LX/LH
- 1000BASE-SX
- 1000BASE-ZX
- 1000BASE-BX10-D
- 1000BASE-BX10-U
- 1000BASE-T
- 100BASE-FX
- CWDM\(^2\)SFP-10G-SR
- SFP-10G-LR

For a complete list of supported SFPs and part numbers, see the data sheet:


### Supported by Minimum Cisco IOS Release

- Cisco IOS Release 12.2(35)SE2
- Cisco IOS Release 12.2(53)SE
### System Requirements

**Table 2** Catalyst 3750-E and 3560-E Switches and Cisco Enhanced EtherSwitch Service Module Supported Hardware (continued)

<table>
<thead>
<tr>
<th>Switch Hardware</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP module patch cable</td>
<td>CAB-SFP-50CM</td>
<td>Cisco IOS Release 12.2(35)SE</td>
</tr>
<tr>
<td>Supports OneX (CVR-X2-SFP10G) and these SFP+ modules</td>
<td>SFP-10G-SR= SFP-10G-LR= SFP-10G-LRM= Only version 02 or later CX1 cables support these SFP modules: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M</td>
<td>12.2(53)SE</td>
</tr>
<tr>
<td>C3K-PWR-1150WAC</td>
<td>1150-W AC power supply module for PoE-capable switches</td>
<td>Supported on all software releases</td>
</tr>
<tr>
<td>C3K-PWR-750WAC</td>
<td>750-W AC power supply module for PoE-capable switches</td>
<td>Supported on all software releases</td>
</tr>
<tr>
<td>C3K-PWR-265WAC</td>
<td>265-W AC power supply module for nonPoE-capable switches</td>
<td>Supported on all software releases</td>
</tr>
<tr>
<td>C3K-PWR-265WDC</td>
<td>265-W DC power supply module for nonPoE-capable switches</td>
<td>Supported on all software releases</td>
</tr>
<tr>
<td>C3K-BLWR-60CFM</td>
<td>Fan module</td>
<td>Supported on all software releases</td>
</tr>
<tr>
<td>Redundant power system (RPS)</td>
<td>Cisco RPS 2300 RPS</td>
<td>Supported on all software releases</td>
</tr>
<tr>
<td>SM-D-ES2-48</td>
<td>48 10/100 ports, 2 SFP module slots</td>
<td>12.2(52)EX</td>
</tr>
<tr>
<td>SM-D-ES3-48-P</td>
<td>48 10/100 ports with PoE, 2 SFP module slots</td>
<td>12.2(52)EX</td>
</tr>
<tr>
<td>SM-D-ES3G-48-P</td>
<td>48 10/100/1000 with PoE, 2 SFP module slots</td>
<td>12.2(52)EX</td>
</tr>
<tr>
<td>SM-ES2-16-P</td>
<td>15 10/100 ports with PoE, 1 10/100/1000 port with PoE</td>
<td>12.2(52)EX</td>
</tr>
</tbody>
</table>
### System Requirements

#### Device Manager System Requirements

#### Hardware

<table>
<thead>
<tr>
<th>Switch Hardware</th>
<th>Description</th>
<th>Supported by Minimum Cisco IOS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM-ES2-24(^7)</td>
<td>23 10/100 ports, 1 10/100/1000 port</td>
<td>12.2(52)EX</td>
</tr>
<tr>
<td>SM-ES2-24-P(^7)</td>
<td>Layer 2-capable, 23 10/100 ports with PoE, 1 10/100/1000 port with PoE</td>
<td>12.2(52)EX</td>
</tr>
<tr>
<td>SM-ES3-16-P(^7)</td>
<td>15 10/100 ports with PoE, 1 10/100/1000 port with PoE</td>
<td>12.2(52)EX</td>
</tr>
<tr>
<td>SM-ES3-24-P(^7)</td>
<td>23 10/100 ports with PoE, 1 10/100/1000 port with PoE</td>
<td>12.2(52)EX</td>
</tr>
<tr>
<td>SM-ES3G-16-P(^7)</td>
<td>16 10/100/1000 ports with PoE</td>
<td>12.2(52)EX</td>
</tr>
<tr>
<td>SM-ES3G-24-P(^7)</td>
<td>24 10/100/1000 ports with PoE</td>
<td>12.2(52)EX</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Processor Speed</th>
<th>DRAM</th>
<th>Number of Colors</th>
<th>Resolution</th>
<th>Font Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>233 MHz minimum(^1)</td>
<td>512 MB(^2)</td>
<td>256</td>
<td>1024 x 768</td>
<td>Small</td>
</tr>
</tbody>
</table>

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

### Software

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

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

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

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

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

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

CNA Compatibility

Cisco IOS 15.0(1)SE will be supported in a future release of the Cisco Network Assistant. Cisco IOS 12.2(35)SE2 and later is only compatible with Cisco Network Assistant 5.0 and later. You can download Cisco Network Assistant from this URL: http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

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

Upgrading the Switch Software

- “Finding the Software Version and Feature Set” section on page 10
- “Deciding Which Files to Use” section on page 11
- “Archiving Software Images” section on page 13
- “Upgrading a Switch by Using the Device Manager or Network Assistant” section on page 13
- “Upgrading a Switch by Using the CLI” section on page 13
- “Recovering from a Software Failure” section on page 14

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.
Upgrading the Switch Software

Note

Although the show version output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the dir filesystem: privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image and a specific software license. If you do not have a service support contract, such as a SMARTnet contract, download the IP base image from Cisco.com. For Catalyst 3750-X and 3560-X switches, this image has the IP base and LAN base feature sets. For Catalyst 3750-E and 3560-E switches, this image has the IP base feature set.

Note

A Catalyst 3750-X or 3560-X switch running the LAN base feature set supports only 255 VLANs.

The switches running the universal software images can use permanent and temporary software licenses. See the “Cisco IOS Software Activation Conceptual Overview” chapter in the Cisco IOS Software Activation Configuration Guide:

The universal software images support multiple feature sets. Use the software activation feature to deploy a software license and to enable a specific feature set.

For information about Catalyst 3750-E and 3560-E software activation, see the Cisco Software Activation and Compatibility Document on Cisco.com:

Catalyst 3750-X and 3560-X switches running payload-encryption images can encrypt management and data traffic. Switches running nonpayload-encryption images can encrypt only management traffic, such as a Secure Shell (SSH) management session.

- Management traffic is encrypted when SSH, Secure Socket Layer (SSL), Simple Network Management Protocol (SNMP), and other cryptographic-capable applications or protocols are enabled.
- Data traffic is encrypted when MACsec is enabled.

For more information about Catalyst 3750-X and 3560-X software licenses and available images, see the Cisco IOS Software Installation Document on Cisco.com:

<table>
<thead>
<tr>
<th>Table 4</th>
<th>Software Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Filenane</td>
</tr>
<tr>
<td>Catalyst 3750-X and Catalyst 3560-X switches</td>
<td></td>
</tr>
<tr>
<td>IP base without payload encryption</td>
<td>c3750e-ipbasek9npe-tar.150-2.SE.tar</td>
</tr>
<tr>
<td></td>
<td>c3560e-ipbasek9npe-tar.150-2.SE.tar</td>
</tr>
</tbody>
</table>
Upgrading the Switch Software

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 4  Software Images (continued)

<table>
<thead>
<tr>
<th>Image</th>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP base with payload encryption</td>
<td>c3750e-ipbasek9-tar.150-2.SE.tar, c3560e-ipbasek9-tar.150-2.SE.tar</td>
<td>Layer 2 and basic Layer 3 features, SSH, SSL, SNMPv3, Kerberos, and MACsec²</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP base image, as well as LAN base image with Layer 2 features</td>
</tr>
<tr>
<td>Universal without payload encryption</td>
<td>c3750e-universalk9npe-tar.150-2.SE.tar, c3560e-universalk9npe-tar.150-2.SE.tar</td>
<td>All the supported universal image features, Kerberos, SSH, SSL, and SNMPv3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LAN base, IP base, and IP services software licenses</td>
</tr>
<tr>
<td>Universal with payload encryption</td>
<td>c3750e-universalk9-tar.150-2.SE.tar, c3560e-universalk9-tar.150-2.SE.tar</td>
<td>All the supported universal image features, Kerberos, SSH, SSL, SNMPv3, and MACsec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LAN base, IP base, and IP services software licenses</td>
</tr>
</tbody>
</table>

**Catalyst 3750-E and Catalyst 3560-E switches**

**IP base image**

|                | c3750e-ipbasek9-tar.150-2.SE.tar, c3560e-ipbasek9-tar.150-2.SE.tar | Layer 2 and basic Layer 3 features, SSH, SSL, SNMPv3, and Kerberos               |

**Universal image**

|                | c3750e-universalk9-tar.150-1.SE.tar, c3560e-universalk9-tar.150-1.SE.tar | All the supported universal image features, Kerberos, SSH, SSL, and SNMPv3      |
|                |                                                                        | IP base and IP services software licenses                                      |

**Cisco enhanced EtherSwitch service modules**

**LAN base image**

|                | c2960sm-lanbasek9-tar.150-2.SE.tar | Layer 2 features, SSH, SNMPv3, and Kerberos                                      |
|                |                                       | For these service modules: SM-D-ES2-48, SM-ES2-16-P, SM-ES2-24, and SM-ES2-24-P. |

**Universal image**

|                | c3560e-universalk9-tar.150-2.SE.tar | All the supported universal image features, Kerberos, SSH, SSL, and SNMPv3    |
|                |                                           | IP base and IP services software licenses                                      |

1. SSH = Secure Shell
2. SSL = Secure Socket Layer
3. SNMPv3 = Simple Network Management Protocol Version 3
4. MACsec = MAC security standard
Archiving Software Images

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

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

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:

**Note**
When you upgrade the switch from Cisco IOS Release 15.0(2)SE to 15.0(2)SE1, a microcode upgrade is started when the switch is reloaded for the first time. The switch may take unusually long to start. We recommend that you download the software on the switch using the `archive download-sw /force-ucode-reload` or `archive download-sw /upgrade-ucode` privileged EXEC command to shorten the reload time of the switch. For more information about using these commands, see the `archive download-sw` command in the Catalyst 3750-X and Catalyst 3560-X Switch Command Reference, Cisco IOS Release 15.0(2)SE and Later guide on Cisco.com:

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:
Upgrading the Switch Software

Step 1
Use Table 4 on page 11 to identify the file that you want to download.

Step 2
Download the software image file:

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

b. Navigate to Switches > LAN Switches - Access

c. Navigate to your switch model.

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

e. Download the image you identified in Step 1.

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

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

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

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

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

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

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

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

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

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

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

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

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

```
Switch# archive download-sw /overwrite
   tftp://198.30.20.19/c3750x-universal-tar.122-55.SE.tar
```

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

Recovering from a Software Failure

For recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.
Installation Notes

Use these methods to assign IP information to your switch:

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

New Software Features

New in Cisco IOS Release 15.0(2)SE5

- Catalyst 3750-X and 3560-X switches now support Universal Power over Ethernet (UPoE).

New in Cisco IOS Release 15.0(2)SE3


Note: This feature is available on the Advanced IP Services feature set.

New in Cisco IOS Release 15.0(2)SE1

- Cisco IOS Release 15.0(1)SE2 on the Catalyst 3750-X and 3560-X switches is now certified under the Federal Information Processing Standard Publication 140-2 (FIPS 140-2) and the Common Criteria for Information Technology Security Evaluation standard (Common Criteria or CC) EAL 2+.
- The command ‘ip tcp adjust-mss’ is not supported on the 3750x/3560x/3750g/3560g/3750e/3560e platforms.
- Cisco IOS Release 15.0(2)SE1 on the Catalyst 3750-X and 3560-X switches has been submitted for certification under FIPS 140-2 and Common Criteria compliance with the US Government, Security Requirements for Network Devices (pp_nd_v1.0), version 1.0, dated 10 December 2010.

Note: The images for the Cisco IOS Release 15.0(2)SE1 on the Catalyst 3750-X and 3560-X switches are FIPS certified. For information about using FIPS certified images, see the “Boot Loader Upgrade and Image Verification for the FIPS Mode of Operation” section in the “Assigning the Switch IP Address and Default Gateway” chapter of the software configuration guide.
FIPS 140-2 is a cryptographic-focused certification, required by many government and enterprise customers, which ensures the compliance of the encryption and decryption operations performed by the switch to the approved FIPS cryptographic strengths and management methods for safeguarding these operations. For more information, see the following links:


Common Criteria is an international standard (ISO/IEC 15408) for computer security certification. This standard is a set of requirements, tests, and evaluation methods that ensures that the Target of Evaluation complies with a specific Protection Profile or custom Security Target. For more information, see the security target document at: http://www.niap-ccewe.org/st/vid10488/.

- Supports reserved entries for IPv6 Security ACEs in Access, Default, Routing, and VLAN templates. You can use IPv6 FHS features such as RA Guard, DHCP Guard, and NDP snooping by using the entries reserved for IPv6 Security Aces.
- Support for Right-To-Use (RTU) licensing, which allows you to upgrade from one license level to another by entering commands in the command line interface without interacting with the Cisco Product License Registration portal.

**New in Cisco IOS Release 15.0(2)SE**

- Support for IOS IPv6 Host mode, which is compliant with the IPv6 Ready Logo Phase-2 Core Protocols test suite. (LAN Base image for Catalyst 3750-X and 3560-X switches; IP Base image for Catalyst 3750-E and 3560-E switches)
- Support for OSPFv3 fast convergence. The OSPFv3 link-state advertisements (LSA) and shortest path first (SPF) throttling feature provides a dynamic method to slow down link-state advertisement updates in OSPFv3 during times of network instability. This feature also allows faster OSPFv3 convergence by providing LSA rate limiting in milliseconds. For more information, see the Configuring IPv6 Unicast Routing chapter of the software configuration guide on Cisco.com. (Switches running the IP Base image)
- Change in the CLI option relating to OSPFv2 LSA rate limiting. The `all` keyword is now removed from the `timers throttle lsa` global configuration command.
- Support for OSPFv3 authentication with IPsec. You can now use the IPsec secure socket API to authenticate OSPF for IPv6 (OSPFv3) packets to ensure that the packets are not altered and resent to the switch. For more information, see the Configuring IPv6 Unicast Routing chapter of the software configuration guide on Cisco.com.
- Support for first hop security (FHS) in IPv6. We support the following functions: IPv6 snooping, IPv6 FHS binding, neighbor discovery protocol (NDP) address gleaning, IPv6 data address gleaning, IPv6 dynamic host configuration protocol (DHCP) address gleaning, IPv6 device tracking, neighbor discovery (ND) Inspection, IPv6 port-based access list, IPv6 DHCP guard, IPv6 router advertisement (RA) guard, IPv6 source guard. For more information, see the Configuring IPv6 Unicast Routing chapter of the software configuration guide on Cisco.com.
- Support for specifying the VLAN to be used for Smart Install Management. The `vstact startup-vlan` command has been added. For more information, see the command reference on Cisco.com.
• Support for IPv6 multicast routing (switches running the IP Services image). For more information, see the Implementing IPv6 Multicast chapter of the software configuration guide on Cisco.com.

• Support for configurable MAC authentication bypass (MAB). You can configure how MAB authentication is performed for client MAC addresses that deviate from the expected standard format or where the RADIUS configuration requires that the user name and password to differ. For more information, see the Configuring IEEE 802.1x Port-Based Authentication chapter in the software configuration guide on Cisco.com.

• Support for TrustSec Secure Group Access (SGA) - Secure Group Tagging (SGT) / Secure Group Access Control List (SGACL). For more information, see the Cisco TrustSec chapter in the software configuration guide. (Catalyst 3750-X and 3560-X switches)

• Support for IKEv2 and IPSecv3 protocols. (IP Base image for Catalyst 3750-X, 3560-X, 3750-E and 3560-E switches)

• Support for Resilient Ethernet Protocol (REP) is added for the IP Base package. REP is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time in ring topologies. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP also supports VLAN load balancing. (IP Base image for Catalyst 3750-X, 3560-X, 3750-E and 3560-E switches.)

• Support for stack power is now extended to the LAN Base license. (Catalyst 3750-X switch)

• Support for Cisco TrustSec SXP version 2, syslog messages, and SNMP support is now extended to the LAN Base license. (Catalyst 3560-X and 3750-X switches)

• Support for port security on Etherchannels. For more information, see the Configuring Port-Based Traffic Control chapter in the software configuration guide.

• Support for IP Source Guard on Etherchannels. For more information, see the Configuring DHCP and IP Source Guard chapter in the software configuration guide.

• Support for SFP-10G-ER (10GBASE-ER SFP+ transceiver module (SMF, 1550-nm, LC duplex connector). (Catalyst 3560-X and 3750-X switches)

### Minimum Cisco IOS Release for Major Features

Table 5 lists the minimum software release after the first release of required to support the major features on the switches. The first release of the Catalyst 3750-X and 3560-X switches was Cisco IOS Release 12.2(53)SE2).

<table>
<thead>
<tr>
<th>Feature</th>
<th>Minimum Cisco IOS Release Required</th>
<th>Catalyst Switch Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical voice VLAN</td>
<td>15.0(1)SE</td>
<td>3750-E, 3560-E 3750-X, 3560-X</td>
</tr>
<tr>
<td>NEAT enhancement to control access to the supplicant port</td>
<td>15.0(1)SE</td>
<td>3750-E, 3560-E 3750-X, 3560-X</td>
</tr>
<tr>
<td>Cisco TrustSec SXP version 2, syslog messages, and SNMP support</td>
<td>15.0(1)SE</td>
<td>3750-E, 3560-E 3750-X, 3560-X</td>
</tr>
<tr>
<td>Auto Smartports improved device classification</td>
<td>15.0(1)SE</td>
<td>3750-E, 3560-E 3750-X, 3560-X</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>Device Sensor</td>
<td>15.0(1)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Built-in Traffic Simulator using Cisco IOS IP SLAs video operations</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Cisco Mediatrace support</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Cisco performance monitor</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>EnergyWise Phase 2.5</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Smart logging</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Protocol storm protection</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>VACL Logging</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Smart Install 3.0</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Auto Smartports enhancements to enable auto-QoS on a digital media</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>player.</td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Memory consistency check routines</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Call Home support</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Support for 16 static routes on SVIs on the LAN Base feature set</td>
<td>12.2(58)SE1</td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>SDM template supporting more indirect routes</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>NTP version 4</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>DHCPv6 bulk-lease query and DHCPv6 relay source configuration</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Rolling stack upgrade</td>
<td>12.2(58)SE1</td>
<td>3750-X, 3750-C</td>
</tr>
<tr>
<td>NSF IETF mode for OSPFv2 and OSPFv3 (IP services feature set)</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>RADIUS, TACACS+, and SSH/SCP over IPv6</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>VRRP for IPv4</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates</td>
<td>12.2(58)SE1</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
</tbody>
</table>
### Table 5 Features Introduced After the First Release 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>Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>AutoSmartports enhancements—support for global macros, last-resort macros, event trigger control, access points, EtherChannels, auto-QoS with Cisco Medianet, and IP phones.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>CDP and LLDP enhancements for exchanging location information with video end points.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Smart Install enhancements including client backup files, zero-touch replacement for clients with the same product-ID, and automatic generation of the image_list file.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Dynamic creation or attachment of an auth-default ACL on a port with no configured static ACLs.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>VLAN assignment on a port configured for multi-auth mode.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>EEM in IP base image.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>IP base support for OSPF routed access.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Cisco TrustSec SXP.</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>Cisco EnergyWise Phase 2 to manage power usage of EnergyWise-enabled Cisco devices and non-Cisco end points running EnergyWise agents</td>
<td>12.2(55)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3750-X, 3560-X</td>
</tr>
<tr>
<td>AutoSmartports enhancements (macro persistency, LLDP-based triggers, MAC address and OUI-based triggers.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>EEM 3.2 Neighbor Discovery, Identity, and MAC-Address-Table.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for IP source guard on static hosts.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>RADIUS Change of Authorization (CoA).</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>802.1x User Distribution to allow deployments with multiple VLANs.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Critical VLAN with multiple-host authentication.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Customizable web authentication enhancement.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Network Edge Access Topology (NEAT) to change the port host mode and apply a standard port configuration on the authenticator switch port.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>VLAN-ID based MAC authentication.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>MAC move to allow hosts to move across ports within the same switch without any restrictions to enable mobility.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>SNMPv3 with Triple Data Encryption Standard (3DES) and 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Hostname inclusion in the option 12 field of DHCPDISCOVER packets.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
</tbody>
</table>
## Table 5  Features Introduced After the First Release 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 enhancement to support the circuit-id sub-option of the</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Option 82 DHCP field.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LLPD-MED enhancements to allow the switch to grant power to the</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>power device (PD), based on the power policy TLV request.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VTP version 3 support.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>QoS marking of CPU-generated traffic and queue CPU-generated traffic</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>on egress ports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEAT with 802.1X switch supplicant, host authorization with CISP, and</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>auto enablement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.1x with open access.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>802.1x authentication with downloadable ACLs and redirect URLs.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Flexible-authentication sequencing to configure the order of</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>authentication methods tried by a port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple-user authentication to allow more than one host to authenticate</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>on an 802.1x-enabled port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supports the LLPD-MED MIB and the CISCO-ADMISSION-POLICY MIB.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Full QoS support for IPv6 traffic.</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Smart Install to allow a single point of management (director) in a</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Medianet to enable intelligent services in the network</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>infrastructure for a wide variety of video applications.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for up to 32 10 Gigabit Ethernet DWDM X2 optical modules.</td>
<td>12.2(52)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Wired location service.</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Connectionless Network Service (CLNS) networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stack troubleshooting enhancements</td>
<td>12.2(50)SE</td>
<td>3750-E</td>
</tr>
<tr>
<td>Support for the Cisco IOS Configuration Engine (previously the Cisco</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>IOS CNS agent)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded Event Manager Version 2.4</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>LLDP-MED network-policy profile time, length, value (TLV).</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>RADIUS server load balancing.</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Auto Smartports Cisco-default and user-defined macros.</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for these MIBs: SCP attribute in the CONFIG_COPY MIB,</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>CISCO-AUTH.FRAMEWORK, CISCO-MAC-AUTH-BYPASS, LLDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 features supported in the IP services and IP base software images:</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>ACLs; DHCPv6 for the DCHP server, client, and relay device; EIGRPv6;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HSRPv6; OSPFv3; RIP; Static routes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 5  Features Introduced After the First Release 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>Generic message authentication support with the SSH Protocol and</td>
<td>12.2(50)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>compliance with RFC 4256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice aware 802.1x and mac authentication bypass (MAB) security</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>violation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local web authentication banner</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for the CISCO-NAC-NAD and CISCO-PAEM MIBs</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Digital Optical Monitoring (DOM) of connected SFP modules</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>The ability to exclude a port in a VLAN from the SVI line-state</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>calculation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HSRP Version 2 (HSRPv2)</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>HSRP for IPv6 (requires the IP services image)</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Disabling MAC address learning on a VLAN</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>PAgP Interaction with Virtual Switches and Dual-Active Detection</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Rehosting a software license and using an embedded evaluation software</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>license</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EOT and IP SLAs EOT static route support</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>DHCP server port-based address allocation</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>DHCP for IPv6 relay, client, server address assignment and prefix</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>delegation (IP services image)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 port-based trust with dual IPv4 and IPv6 SDM templates</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>IPv6 default router preference (DRP)</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Embedded event manager (EEM) for device and system management (IP</td>
<td>12.2(46)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>services only)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP-based autoconfiguration and image update</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Configurable small-frame arrival threshold</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Digital optical monitoring (DOM)</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Source Specific Multicast (SSM) mapping</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>HTTP and HTTP(s) support over IPV6</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>SNMP configuration over IPv6 transport</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>IPv6 support for stateless autoconfiguration</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Flex Link Multicast Fast Convergence</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>IEEE 802.1x readiness check</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>/31 bit mask support for multicast traffic</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Flow-based Switch Port Analyzer (FSPAN)</td>
<td>12.2(44)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Automatic quality of service (QoS) Voice over IP (VoIP) enhancement</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Configuration replacement and rollback</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
</tbody>
</table>
Table 5  
Features Introduced After the First Release 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>Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA)</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Internet Group Management Protocol (IGMP) Helper</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>IP Service Level Agreements (IP SLAs)</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>IP SLAs EOT</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Multicast virtual routing and forwarding (VRF) Lite</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>SSM PIM protocol</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for VRF-aware services</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for the Link Layer Discovery Protocol Media Extensions (LLDP-MED) location TLV</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for the CISCO-MAC-NOTIFICATION-MIB</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for the CISCO-POWER-ETHERNET-EXT-MIB</td>
<td>12.2(40)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>DHCP Snooping Statistics show and clear commands</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>IP phone detection enhancement</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>IP unicast reverse path forwarding (unicast RPF)</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</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-E, 3560-E</td>
</tr>
<tr>
<td>PIM stub routing in the IP base image</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Port security on a PVLAN host</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>VLAN aware port security option</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for auto-rendezvous point (auto-RP) for IP multicast</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>VLAN Flex Link Load Balancing</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Web Cache Communication Protocol (WCCP)</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>SNMP support for the Port Error Disable MIB</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
<tr>
<td>Support for the Time Domain Reflectometry MIB</td>
<td>12.2(37)SE</td>
<td>3750-E, 3560-E</td>
</tr>
</tbody>
</table>

1. Cisco enhanced EtherSwitch service modules do not support Cisco EnergyWise.

Limitations and Restrictions

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

Cisco IOS Limitations

- “Access Control List” section on page 23
Access Control List

- The Catalyst 3560-E and Catalyst 3750-E switches have 964 TCAM entries available for ACLs in the default and routing SDM templates instead of the 1024 entries that are available on the Catalyst 3560 and Catalyst 3750 switches.
  
  There is no workaround. (CSCse33114)

- When a MAC access list is used to block packets from a specific source MAC address, that MAC address is entered in the switch MAC-address table.
  
  The workaround is to block traffic from the specific MAC address by using the `mac address-table static mac-addr vlan vlan-id drop` global configuration command. (CSCse73823)

Address Resolution Protocol

- The switch might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.
  
  The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem. (CSCse06827)

Cisco Redundant Power System 2300

- When connecting the RPS cable between the RPS 2300 and the Catalyst 3750-E or 3560-E switch or other supported network devices, this communication error might appear:
  
  ```bash
  PLATFORM_ENV-1-RPS_ACCESS: RPS is not responding
  ```

  No workaround is required because the problem corrects itself. (CSCsf15170)
Cisco Transceiver Modules and SFP Modules

- (Catalyst 3750-E or 3560-E switches) Switches with the Cisco X2-10GB-LX4 transceiver modules with a version identification number prior to V03 might intermittently fail. The workaround is to use Cisco X2-10GB-LX4 transceiver modules with a version identification number of V03 or later. (CSCsh60076)

- Cisco GLC-GE-100FX SFP modules with a serial number between OPC0926xxxx and OPC0945xxxx might show intermittent module not valid, data, status, link-flapping, and FCS errors. The workaround is to use modules with serial numbers that are not in the specified range. (CSCsh59585)

- When switches are installed closely together and the uplink ports of adjacent switches are in use, you might have problems accessing the SFP module bale-clasp latch to remove the SFP module or the SFP cable (Ethernet or fiber).

  Use one of these workarounds:
  - Allow space between the switches when installing them.
  - In a switch stack, plan the SFP module and cable installation so that uplinks in adjacent stack members are not all in use.
  - Use long, small screwdriver to access the latch then remove the SFP module and cable. (CSCsd57938)

- (Catalyst 3750-E or 3560-E switches) When a Cisco X2-10GB-CX4 transceiver module is in the X2 transceiver module port and you enter the show controllers ethernet-controller tengigabitethernet privileged EXEC command, the command displays some fields as unspecified. This is the expected behavior based IEEE 802.3ae. (CSCsd47344)

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

Configuration

- If a half-duplex port running at 10 Mb/s receives frames with Inter-Packet Gap (IPG) that do not conform to Ethernet specifications, the switch might stop sending packets.

  There is no workaround. (CSCec74610) (Catalyst 3750-X switches)

- When an excessive number (more than 100 packets per second) of Address Resolution Protocol (ARP) packets are sent to a Network Admission Control (NAC) Layer 2 IP-configured member port, a switch might display a message similar to this:

  PLATFORM_RPC-3-MSG_THROTTLED: RPC Msg Dropped by throttle mechanism: type 0, class 51, max_msg 128, total throttled 984323

-Traceback= 6625EC 5DB4C0 5DAA98 55CA80 A2F2E0 A268D8

  No workaround is necessary. Under normal conditions, the switch generates this notification when snooping the next ARP packet. (CSCse47548)

- When there is a VLAN with protected ports configured in fallback bridge group, packets might not be forwarded between the protected ports.

  The workaround is to not configure VLANs with protected ports as part of a fallback bridge group. (CSCsg40322)
When a switch port configuration is set at 10 Mb/s half duplex, sometimes the port does not send in one direction until the port traffic is stopped and then restarted. You can detect the condition by using the `show controller ethernet-controller` or the `show interfaces` privileged EXEC commands.

The workaround is to stop the traffic in the direction in which it is not being forwarded, and then restart it after 2 seconds. You can also use the `shutdown` interface configuration command followed by the `no shutdown` command on the interface. (CSCsh04301)

- When line rate traffic is passing through a dynamic port, and you enter the `switchport access vlan dynamic` interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

The workaround is to enter the `switchport access vlan dynamic` interface configuration command separately on each port. (CSCsi26392)

- (Catalyst 3750-X or 3750-E switches) If you enter the `show tech-support` privileged EXEC command after you enter the `remote command {all | stack-member-number}` privileged EXEC command, the complete output does not appear.

The workaround is to use the `session stack-member-number` privileged EXEC command. (CSCsz38090)

- (Catalyst 3750-X or 3560-X switches) When the switch flash memory has less than 6 MB free space, there is not enough space in flash memory to hold temporary files created as part of a microcontroller unit (MCU) image upgrade, and the upgrade fails.

The workaround is to delete any unnecessary files in flash memory, delete the temporary files created as part of the failed upgrade, and try the MCU upgrade again. (CSCtd75400)

- Identity Services Engine (ISE) is not available on Catalyst 2000 series switches.

- The `device-sensor accounting` global configuration command is not available on Catalyst 2000 series switches.

### Diagnostics

- (Catalyst 3750-X or 3560-X switches) When you enter the `test cable-diagnostics tdr interface` or the `show cable-diagnostics tdr interface` privileged EXEC command on an interface to determine the length of a connected cable, the cable length might be reported as N/A. This can occur when there is no link, a 10 Mb/s link, or a 100 Mb/s link, even though there are no cable faults. Cable length is reported correctly when a 1 Gb/s link is active on the interface.

The workaround to verify the cable length is to enter the commands when a Gigabit link is active on the interface or after disconnecting the far end of the cable. (CSCte43869)

### EtherChannel

- In an EtherChannel running Link Aggregation Control Protocol (LACP), the ports might be put in the suspended or error-disabled state after a stack partitions or a member switch reloads. This occurs when:
  - The EtherChannel is a cross-stack EtherChannel with a switch stack at one or both ends.
  - The switch stack partitions because a member reloads. The EtherChannel is divided between the two partitioned stacks, each with a stack master.
The EtherChannel ports are put in the suspended state because each partitioned stack sends LACP packets with different LACP Link Aggregation IDs (the system IDs are different). The ports that receive the packets detect the incompatibility and shut down some of the ports. Use one of these workarounds for ports in this error-disabled state:

- Enable the switch to recover from the error-disabled state.
- Enter the `shutdown` and the `no shutdown` interface configuration commands to enable the port.

The EtherChannel ports are put in the error-disabled state because the switches in the partitioned stacks send STP BPDUs. The switch or stack at the other end of the EtherChannel receiving the multiple BPDUs with different source MAC addresses detects an EtherChannel misconfiguration. After the partitioned stacks merge, ports in the suspended state should automatically recover. (CSCse33842)

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

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

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

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

  There is no workaround. (CSCsh12472)

### IEEE 802.1x Authentication

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

  Use one of these workarounds (CSCsd90495):

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

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

  - If the connected device is supposed to be unauthorized, the connected device might be authorized on the VLAN that is assigned to the critical port instead of to a guest VLAN.
  - If the device is supposed to be authorized, it is authorized on the VLAN that is assigned to the critical port.
Use one of these workarounds (CSCse04534):

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

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

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

**Multicasting**

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

The workaround is to not generate multicast packets with a TTL value of 0 or 1, or disable multicast routing in the VLAN. (CSCeh21660)

- Multicast packets denied by the multicast boundary access list are flooded in the incoming VLAN when all of these conditions are met:
  - Multicast routing is enabled in the VLAN.
  - The source IP address of the multicast packet belongs to a directly connected network.
  - The packet is denied by the IP multicast boundary access-list configured on the VLAN.

There is no workaround. (CSCei08359)

- Reverse path forwarding (RPF) failed multicast traffic might cause a flood of Protocol Independent Multicast (PIM) messages in the VLAN when a packet source IP address is not reachable.

The workaround is to not send RPF-failed multicast traffic, or make sure that the source IP address of the RPF-failed packet is reachable. (CSCsd28944)

- If the `clear ip mroute` privileged EXEC command is used when multicast packets are present, it might cause temporary flooding of incoming multicast traffic in the VLAN.

There is no workaround. (CSCsd45753)

- When you configure the `ip igmp max-groups number` and `ip igmp max-groups action replace` interface configuration commands and the number of reports exceed the configured max-groups value, the number of groups might temporarily exceed the configured max-groups value. No workaround is necessary because the problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)

- When you configure the IGMP snooping throttle limit by using the `ip igmp max-groups number` interface configuration on a port-channel interface, the groups learned on the port-channel might exceed the configured throttle limit number, when all of these conditions are true:
  - The port-channel is configured with member ports across different switches in the stack.
  - When one of the member switches reloads.
  - The member switch that is reloading has a high rate of IP IGMP joins arriving on the port-channel member port.
The workaround is to disable the IGMP snooping throttle limit by using the `no ip igmp max-groups number` interface configuration command and then to reconfigure the same limit again. (CSCse39909)

**PoE or PoE+**

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

- The Cisco 7905 IP Phone is error-disabled when the phone is connected to an external power source. The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

- The `pethPsePortShortCounter` MIB object appears as *short* even though the powered device is powered on after it is connected to the PoE port.
  
  There is no workaround. (CSCsg20629)

- (Catalyst 3750-X or 3560-X switches) When a powered device (such as an IP phone) connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the switch locks to the power-negotiation protocol of that first packet. The switch does not respond to power requests from the other protocol. For example, if the switch is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the switch has locked on it, the switch does not respond to LLDP power requests and can no longer power on any accessories.
  
  The workaround is to turn the powered device off and then on again.

**QoS**

- When QoS is enabled and the egress port receives pause frames at the line rate, the port cannot send packets.
  
  There is no workaround. (CSCeh18677)

- Egress shaped round robin (SRR) sharing weights do not work properly with system jumbo MTU frames.
  
  There is no workaround. (CSCsc63334)

- In a hierarchical policy map, if the VLAN-level policy map is attached to a VLAN interface and the name of the interface-level policy map is the same as that for another VLAN-level policy map, the switch rejects the configuration, and the VLAN-level policy map is removed from the interface.
  
  The workaround is to use a different name for the interface-level policy map. (CSCsd84001)

- If the ingress queue has low buffer settings and the switch sends multiple data streams of system jumbo MTU frames at the same time at the line rate, the frames are dropped at the ingress.
  
  There is no workaround. (CSCsd72001)

- When you use the `srr-queue bandwidth limit` interface configuration command to limit port bandwidth, packets that are less than 256 bytes can cause inaccurate port bandwidth readings. The accuracy is improved when the packet size is greater than 512 bytes.
  
  There is no workaround. (CSCsg79627)
• If QoS is enabled on a switch and the switch has a high volume of incoming packets with a maximum transmission unit (MTU) size greater than 1512 bytes, the switch might reload.

Use one of these workarounds:
- Use the default buffer size.
- Use the `mls qos queue-set output qset-id buffers allocation1 ... allocation4` global configuration command to allocate the buffer size. The buffer space for each queue must be at least 10 percent. (CSCsx69718) (Catalyst 3750-X switches)

• If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

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

There is no impact to switch functionality.
There is no workaround. (CSCtg32101)

**RADIUS**

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

**Routing**

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

The workaround is to reduce the number of OSPF neighbors to 200 or less. (CSCse65252)

• When the PBR is enabled and QoS is enabled with DSCP settings, the CPU utilization might be high if traffic is sent to unknown destinations.

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

**Smart Install**

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

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

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

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

• Backing up a Smart Install configuration could fail if the backup repository is a Windows server and the backup file already exists in the server.
The workaround is to use the TFTP utility of another server instead of a Windows server or to manually delete the existing backup file before backing up again. (CSCte53737)

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

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

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

- If the director in the Smart Install network is located between an access point and the DHCP server, the access point tries to use the Smart Install feature to upgrade even though access points are not supported devices. The upgrade fails because the director does not have an image and configuration file for the access point.

There is no workaround. (CSCtg98656)

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

There is no workaround. (CSCth35152)

**SPAN and RSPAN**

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

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

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

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

- (Catalyst 3750-E or 3560-E switches) The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

The workaround is to configure aggressive UDLD. (CSCsh70244).
- (Catalyst 3560-X and 3750-X switches) When you enter the `show monitor` privileged EXEC command the monitor source port output is incorrect. This situation occurs only if the monitor source port(s) is a pluggable Gigabit module and you set any source port combination, except when just using a single Gigabit port on the pluggable module as the source port.

  This is a cosmetic issue and the workaround is to use the `show platform monitor session` privileged EXEC command to display the correct source ports. (CSCtn67868)

**Spanning Tree Protocol**

- CSCtl60247

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

  There is no workaround.

- CSCuz14346

  The Root port gets stuck into BLK state when the secondary root bridge priority is decreased to less than the current root bridge priority under RSTP mode.

  Below are the scale numbers for n-number of stacks to avoid “CSCuz14346”

  - For 8 member stack: Maximum number of active vlan that can be configured without seeing any SPT issue is 46.
  - For 7 member stack: Maximum number of active vlan that can be configured without seeing any SPT issue is 60.
  - For 6 member stack: Maximum number of active vlan that can be configured without seeing any SPT issue is 70.
  - For 5 member stack: Maximum number of active vlan that can be configured without seeing any SPT issue is 80.

  The Workaround is to:

  - Shut/No shut the effected port.
  - For vlan numbers beyond the scale number mentioned above, please use the MST mode.

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

- When a switch stack is running 802.1x single host mode authentication and has filter-ID or per-user policy maps applied to an interface, these policies are removed if a master switchover occurs. Even though the output from the `show ip access-list` privileged EXEC command includes these ACLs, the policies are not applied.

  The workaround it to enter a `shutdown` and then a `no shutdown` interface configuration command on the interface. (CSCsx70643)
- Where there is a mixed hardware stack with Catalyst 3750-X or Catalyst 3750-E and 3750 switches as stack members, when you change the configuration and enter the `write memory` privileged EXEC command, the `unable to read config` message appears.

  The workaround is to wait a few seconds and then to reenter the `write memory` privileged EXEC command. (CSCsd66272)

- When using the `logging console` global configuration command, low-level messages appear on both the stack master and the stack member consoles.

  The workaround is to use the `logging monitor` global configuration command to set the severity level to block the low-level messages on the stack member consoles. (CSCsd79037)

- In a mixed stack which consists of Catalyst 3750 switches along with Catalyst 3750-X or Catalyst 3750-E switches, when the stack ring is congested with approximately 40 Gb/s of traffic, some of the local traffic from one port to another on a Catalyst 3750-X or 3750-E member might be dropped.

  The workaround is to avoid traffic congestion on the stack ring. (CSCsd87538)

- If a new member switch joins a switch stack within 30 seconds of a command to copy the switch configuration to the running configuration of the stack master, the new member might not get the latest running configuration and might not operate properly.

  The workaround is to reboot the new member switch. Use the `remote command all show run` privileged EXEC command to compare the running configurations of the stack members. (CSCsf31301)

- When the flash memory of a stack member is almost full, it might take longer to start up than other member switches. This might cause that switch to miss the stack-master election window. As a result, the switch might fail to become the stack master even though it has the highest priority.

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

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

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

- A stack member switch might fail to bundle Layer 2 protocol tunnel ports into a port channel when you have followed these steps:

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

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

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

  ```
  Switch(config)# interface fastethernet1/0/11
  Switch(config-if)# l2protocol-tunnel cdp
  Switch(config-if)# channel-group 1 mode on (CSCsk96058)
  ```

- After a stack bootup, the spanning tree state of a port that has IEEE 802.1x enabled might be blocked, even when the port is in the authenticated state. This can occur on a voice port where the Port Fast feature is enabled.
Limitations and Restrictions

The workaround is to enter a **shutdown** interface configuration command followed by a **no shutdown** command on the port in the blocked state. (CSCs164124)

- When the switch stack is in the HSRP active state and a master changeover occurs, you cannot ping the stack by using an HSRP virtual IP address.
  There is no workaround. (CSCth00938)
- In a stackable switch, if VRF configuration is changed and this is followed by a master switchover, VRF stops working.
  The workaround is to reload the switch stack after the VRF configuration is changed. (CSCtn71151)

**Stack Power (Catalyst 3750-X only)**

- When a power stack has been configured in redundant mode, which is not the default, and then split by either removing cables or disabling StackPower ports, the newly created power stack has the same mode as the former power stack, but this is not shown in the configuration file.
  The workaround when you are forming power stack topologies if the power stack mode is not the default (power sharing), you should also configure the power stack mode on the new power stacks by entering the **mode redundant** power-stack configuration command. (CSCte33875)

**VLANs**

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.
  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)
- When the domain is authorized in the guest VLAN on a member switch port without link loss and an Extensible Authentication Protocol over LAN (EAPOL) is sent to an IEEE 802.1x supplicant to authenticate, the authentication fails. This problem happens intermittently with certain stacking configurations and only occurs on the member switches.
  The workaround is to enter the **shut** and **no shut** interface configuration commands on the port to reset the authentication status. (CSCsf98557)
- The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:
  - IEEE 802.1 is enabled.
  - A supplicant is authenticated on at least one port.
  - A new member joins a switch stack.
  You can use one of these workarounds:
    - Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.
    - Remove and reconfigure the VLAN. (CSCsi26444)
- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.
  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** `timeout-value` command. (CSCsk65142)
Limitations and Restrictions

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

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

**TrustSec**

The following guidelines and limitations apply to configuring Cisco TrustSec SGT and SGACL on the Catalyst 3750-X/3560-X switch:

- You cannot statically map an IP-subnet to an SGT. You can only map IP addresses to an SGT. When you configure IP address-to-SGT mappings, the IP address prefix must be 32.

- If a port is configured in Multi-Auth mode, all hosts connecting on that port must be assigned the same SGT. When a host tries to authenticate, its assigned SGT must be the same as the SGT assigned to a previously authenticated host. If a host tries to authenticate and its SGT is different from the SGT of a previously authenticated host, the VLAN port (VP) to which these hosts belong is error-disabled.

- Cisco TrustSec enforcement is supported only on up to eight VLANs on a VLAN-trunk link. If there are more than eight VLANs configured on a VLAN-trunk link and Cisco TrustSec enforcement is enabled on those VLANs, the switch ports on those VLAN-trunk links will be error-disabled.

- The switch cannot assign an SGT based on SXP listening; it can only forward the SXP bindings through the SXP protocol.

- Port-to-SGT mapping can be configured only on Cisco TrustSec links (that is, switch-to-switch links). Port-to-SGT mapping cannot be configured on host-to-switch links.

  When port-to-SGT mapping is configured on a port, an SGT is assigned to all ingress traffic on that port. There is no SGACL enforcement for egress traffic on the port.

- SGT/SGACL is supported on Cisco Catalyst 3750-X and 3560-X series switches with all network uplink modules: C3KX-NM-1G, C3KX-NM-10G, C3KX-NM-10GT and C3KX-SM-10G. The C3KX-SM-10G is only required for MACsec on the uplinks.

**Device Manager Limitations**

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

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

**Hardware Limitations**

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

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

  There is no workaround. (CSCtt05810)

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

- “Switch Stack Notes” section on page 35
- “Control Plane Protection” section on page 35
- “Cisco IOS Notes” section on page 35
- “Device Manager Notes” section on page 36

Switch Stack Notes

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

Control Plane Protection

Catalyst 3750-X, 3750-E, 3560-X and 3560-E switches internally support up to 16 different control plane queues. Each queue is dedicated to handling specific protocol packets and is assigned a priority level. For example, STP, routed, and logged packets are sent to three different control plane queues, which are prioritized in corresponding order, with STP having the highest priority. Each queue is allocated a certain amount of processing time based on its priority. The processing-time ratio between low-level functions and high-level functions is allocated as 1-to-2. Therefore, the control plane logic dynamically adjusts the CPU utilization to handle high-level management functions as well as punted traffic (up to the maximum CPU processing capacity). Basic control plane functions, such as the CLI, are not overwhelmed by functions such logging or forwarding of packets.

Cisco IOS Notes

- Unlike other platforms, the response to an Energywise query on a Catalyst 3750-X or 3560-X is the actual switch power consumption and not a fixed number.
- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

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

If this message appears, make sure that there is network connectivity between the switch and the ACS. You should also make sure that the switch has been properly configured as an AAA client on the ACS.
• If the switch has interfaces with automatic QoS for voice over IP (VoIP) configured and you upgrade the switch software, when you enter the `auto qos voip cisco-phone` interface configuration command on another interface, you might see this message:

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

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

**Device Manager Notes**

• You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.

• When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.

• For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese.

• We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

From Microsoft Internet Explorer:

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

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

If you are not using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.
Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

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

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

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

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

### Cisco Bug Search Tool

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

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

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

### Open Caveats

Unless otherwise noted, these caveats apply to Catalyst 3750-X, 3750-E, 3560-X, and 3560-E switches

- CSCug96267 (Catalyst 3750-X, 3560-X, and 3750-E switches)
When Catalyst 3k switch stack is not configured as rep edge and is just part of the ring, it causes convergence of about 4 to 8 seconds for some streams.

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 overwitten by the director and the client receives the image and configuration that the director sends.

Use one of these workarounds:

- If client needs to upgrade using an image and configuration file configured in the DHCP server options, you should remove the client from the Smart Install network during the upgrade.
- In a network using Smart Install, you should not configure options for image and configuration in the DHCP server. For clients to upgrade using Smart Install, you should configure product-id specific image and configuration files in the director.

- CSCtf79259 (Catalyst 3750-X or 3560-X switches)

If you install 10/100/1000BASE-TX or 100BASE-FX SFPs in the SFP+ module ports (port 2 or port 4), the ports are put in an error disabled state. These SFPs are not supported in the SFP+ ports.

There is no workaround.

- CSCtg35226 (Catalyst 3750-X or 3750-E switches)

Cisco Network Assistant displays the LED ports with a light blue color for all switches in a stack that have the Catalyst 3750G-48PS switch as part of the stack.

There is no workaround.

- CSCtj97806

Mediatrace does not report statistics on the initiator under these conditions:

- The responder is a mixed switch stack with a Catalyst 3750 as the master switch
- The ingress interface on the responder from the initiator is on a member switch.

The workaround is to ensure that the mediatrace ingress and egress connections are on the stack master or to configure a Catalyst 3750-E or 3750-X as the stack master and then reload the switch stack.

- CSCtn46265 (Catalyst 3560-X and 3750-X switches)

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

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

- CSCtq35006

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

There is no workaround. The dropped entries are removed when the IP phone is reauthenticated.
- **CSCtq76989 (Catalyst 3750-X or 3560-X switch)**
  A *seed* switch is connected to a RADIUS server either directly or through a trunk port. A *non-seed switch* authenticates with the RADIUS server through the *seed* switch, based on the credential information defined in the RADIUS server. Cisco TrustSec (CTS) parameters must be configured on both the *seed* switch and the *non-seed* switch trunk interfaces.

  Although the *non-seed* switch is authenticated and authorized to connect to the network, supplicant devices connected to the *non-seed* switch might be unable to connect to the network, under these circumstances:
  - CTS caching is enabled on the *seed* switch and not enabled on the *non-seed* switch.
  - The *seed* switch reported the 802.1x role of the *non-seed* switch CTS trunk as authenticator in multi-host mode.
  - The *non-seed* switch reported this CTS trunk as the 802.1x authenticator role in single host mode and as supplicant.

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

- **CSCtr87645**
  ASP now uses a device classifier, which determines the type of device that is connected to the switch. As a result, ASP has no control over the protocol type that is used to detect the device. Therefore, the protocol detection controls are deprecated. When you enter the *macro auto global control detection* command, the protocol does not show up in the running configuration; however, the *filter-spec* command is shown in the output.

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

- **CSCtt22566 (Catalyst 3560-X and 3750-X switches)**
  Monitored SPAN traffic is not sent to the SPAN destination when TrustSec MACsec is enabled on the SPAN source interface.

  There is no workaround.

- **CSCty02174 (Catalyst 3750-X switch)**
  A stack power member switch that does not have a PSU connected in Slot A or Slot B might fail during a Cisco IOS upgrade.

  - The workaround is to ensure that each stack member has at least one PSU connected.

  Alternatively, you can download and install the Cisco IOS image using the *archive download-sw /force-ucode-reload* privileged EXEC command.

- **CSCua22035**
  The following message may be erroneously displayed during the boot up process.

  ```
  Message "stack locked up.. even after FSM reset"
  ```

  There is no workaround.

- **CSCua58659**
  The global *power inline consumption default 15400* command fails to restrict the power consumption of a PoE+ port 15.4 W.
The workaround is to use the **power inline consumption 15400** command in interface configuration mode.

- CSCub20474
  In a switch stack, multicast traffic can be lost for up to 60 seconds when the master switch is reloaded. Because the platform does not support multicast non-stop-forwarding (NSF), the time before traffic reconvergence after a switchover can vary.
  
  There is no workaround.

- CSCuc95496 (Catalyst 3750-E and 3560-E switches)
  Catalyst 3560E switches crash frequently on the latest Cisco releases IOS 12.2(58)SE2 and 15.0(2)SE.
  
  There is no known workaround.

- CSCug81202
  When the `show sdm prefer` command is run on the switch, the template displays the number of indirect IPv4 routes as 7.875K instead of 8K compared to Cisco IOS Release 15.0(2)SE2. There is a reduction of 0.125K in the desktop routing template.
  
  There is no workaround.

- CSCui89695 (Catalyst 3750-X and 3750-E switches)
  When sampled NetFlow is configured with the command `ip flow monitor fm-3 in`, the sampler tables are not exported to the collector.
  
  The workaround is to use the configuration command `ip flow monitor fm-3 sampler s-1 in`.

- CSCui96470
  While configuring VLAN load balancing using Resilient Ethernet Protocol (REP) on ether channel interface where bundled interfaces are spread across member stack switches, the MAC address flaps when the ether channel state changes from open to alternate.
  
  There is no workaround.

- CSCvm20678
  Inline POE-3K: 'oper police' shows 'n/a' instead 'ok' in police errdisable
  
  There is no workaround.

---

**Resolved Caveats**

- Caveats Resolved in Cisco IOS Release 15.0(2)SE13, page 41
- Caveats Resolved in Cisco IOS Release 15.0(2)SE12, page 41
- Caveats Resolved in Cisco IOS Release 15.0(2)SE11, page 42
- Caveats Resolved in Cisco IOS Release 15.0(2)SE10, page 43
- Caveats Resolved in Cisco IOS Release 15.0(2)SE9, page 43
- Caveats Resolved in Cisco IOS Release 15.0(2)SE8, page 44
- Caveats Resolved in Cisco IOS Release 15.0(2)SE7, page 45
- Caveats Resolved in Cisco IOS Release 15.0(2)SE6, page 52
- Caveats Resolved in Cisco IOS Release 15.0(2)SE5, page 58
Caveats Resolved in Cisco IOS Release 15.0(2)SE13

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to https://tools.cisco.com/bugsearch/.

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuq41114</td>
<td>ENH: SSH configuration option to restrict cipher public key and HMAC</td>
</tr>
<tr>
<td>CSCva46459</td>
<td>SSH session hangs if it is not closed properly</td>
</tr>
<tr>
<td>CSCux86075</td>
<td>Unexpected crash during SSH operation</td>
</tr>
<tr>
<td>CSCvj25124</td>
<td>Cisco IOS and IOS XE Software Cluster Management Protocol Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvj25068</td>
<td>Cisco IOS and IOS XE Software Cluster Management Protocol Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCvj98575</td>
<td>Cisco IOS and IOS XE HSRPv2 Information Leak Vulnerability</td>
</tr>
</tbody>
</table>

Caveats Resolved in Cisco IOS Release 15.0(2)SE12

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to https://tools.cisco.com/bugsearch/.

<table>
<thead>
<tr>
<th>Caveat ID Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsv05154</td>
<td>Cisco IOS HTTP server vulnerable to CSRF attacks</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>CSCuj73916</td>
<td>Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCur29331</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>CSCut50727</td>
<td>Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities</td>
</tr>
<tr>
<td>CSCuu76493</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 15.0(2)SE11

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to https://tools.cisco.com/bugsearch/.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCsy56638</td>
<td>Switch crashes after getnext on the last cafServerAliveAction index</td>
</tr>
<tr>
<td>CSCvd48893</td>
<td>Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability</td>
</tr>
<tr>
<td>CSCve60507</td>
<td>Crash in &quot;mac auth bypass&quot; SNMP code</td>
</tr>
<tr>
<td>CSCsm45390</td>
<td>DHCP relay security vulnerability</td>
</tr>
<tr>
<td>CSCva37748</td>
<td>When enable ip source guard, a part of the clients cannot communicate</td>
</tr>
<tr>
<td>CSCuw77959</td>
<td>1801M - %DATACORRUPTION-1-DATAINCONSISTENCY: copy error</td>
</tr>
<tr>
<td>CSCuz81292</td>
<td>IPv6 neighbor discovery packet processing behavior</td>
</tr>
<tr>
<td>CSCva74756</td>
<td>OSPF Rogue LSA with maximum sequence number vulnerability</td>
</tr>
</tbody>
</table>

Caveats Resolved in Cisco IOS Release 15.0(2)SE10a

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to https://tools.cisco.com/bugsearch/.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuu13476</td>
<td>Cisco IOS &amp; IOS XE Software OpenSSH TCP Denial of Service Vulnerability</td>
</tr>
<tr>
<td>CSCuu43892</td>
<td>Switch crashes on qpair_full after executing dhcpd_* functions</td>
</tr>
</tbody>
</table>
Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.0(2)SE10

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to https://tools.cisco.com/bugsearch/.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvb16274</td>
<td>PPTP Start-Control-Connection-Reply packet leaks router memory</td>
</tr>
<tr>
<td>CSCvb29204</td>
<td>BenignCertain on IOS and IOS-XE</td>
</tr>
<tr>
<td>CSCum45713</td>
<td>UUT crashed for scale session</td>
</tr>
<tr>
<td>CSCuo95194</td>
<td>Switch fails while copying a configuration file to running-config using RCP</td>
</tr>
<tr>
<td>CSCus21950</td>
<td>Crash seen after getting LINEPROCDEAD errors and tracebacks</td>
</tr>
<tr>
<td>CSCuw71809</td>
<td>No warning message when switch configures “ip tcp adjust-mss”</td>
</tr>
<tr>
<td>CSCux19111</td>
<td>IGMP reports dropped on Standby ISE dACL is not being matched</td>
</tr>
<tr>
<td>CSCux31188</td>
<td>Shutdown is displayed with linkup channel member port on show run.</td>
</tr>
<tr>
<td>CSCux38041</td>
<td>Broadcast packet does not send when port channel changes to normal port</td>
</tr>
<tr>
<td>CSCux48069</td>
<td>Switch fails to apply DACL after master reload</td>
</tr>
<tr>
<td>CSCux57150</td>
<td>RSTP Message Age exceeds Max Age of 20</td>
</tr>
<tr>
<td>CSCux62169</td>
<td>OIL Pruned on Last Hop Router by IGMPv2 Leave</td>
</tr>
<tr>
<td>CSCux81884</td>
<td>RADIUS server failover leaves port in inconsistent state</td>
</tr>
<tr>
<td>CSCuy33215</td>
<td>Cannot apply REP config under portchannel after initial boot up</td>
</tr>
<tr>
<td>CSCuz14346</td>
<td>(3750-X, 3750-E) Root Port gets stuck in BLK state after changing the Root Bridge</td>
</tr>
</tbody>
</table>

Caveats Resolved in Cisco IOS Release 15.0(2)SE9

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to https://tools.cisco.com/bugsearch/.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCtn75051</td>
<td>%SYS-3-TIMERNEG: Cannot start timer with negative offset</td>
</tr>
<tr>
<td>CSCul01067</td>
<td>Memory leak in NTP client with IPv6 configuration</td>
</tr>
<tr>
<td>CSCuq53377</td>
<td>AAA AttrL memory Leak due to Auth-Manager</td>
</tr>
<tr>
<td>CSCus13476</td>
<td>CSR handled only one MACSec interface's authentication</td>
</tr>
<tr>
<td>CSCus40723</td>
<td>No simulated EAP success message to the client for credential failure</td>
</tr>
</tbody>
</table>
Resolved Caveats

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to https://tools.cisco.com/bugsearch/.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCu60629</td>
<td>unauth timer not taking effect when configured on the fly</td>
</tr>
<tr>
<td>CSCut20271</td>
<td>C3560X responds to ARP request from management port</td>
</tr>
<tr>
<td>CSCut64281</td>
<td>Ports on Member of the stack takes long time to learn/age MAC addr</td>
</tr>
<tr>
<td>CSCu16044</td>
<td>3750 - Not Processing LACP PDUs if Native VLAN is not created</td>
</tr>
<tr>
<td>CSCuu28768</td>
<td>C2960 ARP Table adding MACs on Incorrect Interface</td>
</tr>
<tr>
<td>CSCuu41771</td>
<td>Members in a 2960 cluster unable to save configuration in IOS 15.x</td>
</tr>
<tr>
<td>CSCuu47539</td>
<td>(3750-X) Stack port becomes root port after reload on 3750X</td>
</tr>
<tr>
<td>CSCuu59206</td>
<td>(3560-X) LHR generates duplicate mcast packets</td>
</tr>
<tr>
<td>CSCuu9332</td>
<td>Frame with special DesMac is forwarded by STP block port</td>
</tr>
<tr>
<td>CSCuv05123</td>
<td>c3560e/v151_sy_throttle platform doesn't store NTP drift values properly</td>
</tr>
<tr>
<td>CSCuv53430</td>
<td>(3750-X) Inconsistent VLAN BDPU received on uplink L3 switch</td>
</tr>
<tr>
<td>CSCuv94875</td>
<td>SmartPort Macro with SCP not working</td>
</tr>
</tbody>
</table>

### Caveats Resolved in Cisco IOS Release 15.0(2)SE8

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to https://tools.cisco.com/bugsearch/.

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCut53358</td>
<td>SM-D-ES3G-48-P Will not supply 20W of Power</td>
</tr>
<tr>
<td>CSCuq06556</td>
<td>SM-ES3G-24-P: Hardware limitation has reached for policymap</td>
</tr>
<tr>
<td>CSCtq29263</td>
<td>Netflow: Exporter source interface issue.</td>
</tr>
<tr>
<td>CSCut13064</td>
<td>BPDU filter not work on output port when disable STP</td>
</tr>
<tr>
<td>CSCue03754</td>
<td>Crash while route is getting cleared</td>
</tr>
<tr>
<td>CSCuq67809</td>
<td>3750x stack crashes with to big buffer allocated</td>
</tr>
<tr>
<td>CSCuq11337</td>
<td>Fail to bundle l2protocol ports into channel</td>
</tr>
<tr>
<td>CSCur94665</td>
<td>Switch crashes with multicast routing enabled when TCN timer expires.</td>
</tr>
<tr>
<td>CSCuj31600</td>
<td>Call Home cases stack member crash.</td>
</tr>
<tr>
<td>CSCus36457</td>
<td>C3750x expires Mroute when forwarding low traffic rate.</td>
</tr>
<tr>
<td>CSCup86619</td>
<td>Port err-disable after link-flap with &quot;speed nonegotiate&quot; option.</td>
</tr>
<tr>
<td>CSCur09936</td>
<td>C3750X stack packet loss on Channel interface when removed backup int.</td>
</tr>
<tr>
<td>CSCur64486</td>
<td>Switch is unable to send packets with payload larger than 1496 bytes.</td>
</tr>
<tr>
<td>CSCtq21722</td>
<td>SNMP crash forced due to an invalid memory block</td>
</tr>
</tbody>
</table>
### Caveats Resolved in Cisco IOS Release 15.0(2)SE7

- **CSCef59635**
  Telnet sessions that are incompletely established may not time out after a period of inactivity, leading to eventual exhaustion of available VTY lines.

  When the telnet client initiates a telnet session to IOS Server with a small TCP window size (<2) (rcvwnd in the client tcp, sndwnd in the server side), the target lines are hung for ever. It needs to be manually cleared via clear tcp only (clear line does not work). This issue happens for both VTY/TTY sessions.

  The workaround is that it needs to be manually cleared via clear tcp tcb 0xXXXX only (clear line does not work).

  0xXXXX corresponds to hung line.

- **CSCsk88751**

### Resolved Caveats

<table>
<thead>
<tr>
<th>Bug ID</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuo66933</td>
<td>Switch sent Failure packet after reboot and caused PC to fail authenticate</td>
</tr>
<tr>
<td>CSCue80816</td>
<td>Crash while routine config push through SNMP</td>
</tr>
<tr>
<td>CSCud65150</td>
<td>Crash after Kron runs a TCL script</td>
</tr>
<tr>
<td>CScIx23014</td>
<td>HSRP hellos cannot be sourced from certain IPs for specific vlan</td>
</tr>
<tr>
<td>CSCuo31164</td>
<td>match prefix is removed from SNMP V3 configuration after host command</td>
</tr>
<tr>
<td>CSCum75962</td>
<td>abnormal dot1x authentication failure msg from some specific mac address</td>
</tr>
<tr>
<td>CSCuo85748</td>
<td>dot1x authorization fails, when we recovering from Guest VLAN</td>
</tr>
<tr>
<td>CSCum65703</td>
<td>Inconsistency on config &quot;privilege&quot; commands as seen in running-config</td>
</tr>
<tr>
<td>CSCsq42459</td>
<td>No log message of falling the cpu threshold</td>
</tr>
<tr>
<td>CSCuh46221</td>
<td>EEM Tcl policies fail due to false out of memory error</td>
</tr>
<tr>
<td>CScj717637</td>
<td>MF: HTTPS generates a new self-signed cert on reboot even if one exists</td>
</tr>
<tr>
<td>CSCud66899</td>
<td>IOS supplicant: ACS5 authc fail for PEAPv1/MSCHAPv2</td>
</tr>
<tr>
<td>CSCur58372</td>
<td>&quot;snmp-server enable traps syslog&quot; still in &quot;show run all&quot; after removal</td>
</tr>
<tr>
<td>CSCui43116</td>
<td>dot1x State Radius AV pair not send while failing over between AAA grps</td>
</tr>
<tr>
<td>CSCur76305</td>
<td>Memory leak in ASP proces Catalyst 2960s</td>
</tr>
<tr>
<td>CSCuq10827</td>
<td>C3560X cHsrpGrpStandbyState is incorrect</td>
</tr>
<tr>
<td>CSCur50403</td>
<td>LOGIN_FAILED log message should not display the bad username</td>
</tr>
<tr>
<td>CSCur74187</td>
<td>Device sending Client IP address as &quot;Calling-Station-Id&quot; with WebAuth</td>
</tr>
<tr>
<td>CSCut05808</td>
<td>UDP(1975) causes Error msg %IPC-2-INVALIDZONE</td>
</tr>
</tbody>
</table>
The process **Kron CLI Process show tech-support password | redirect tftp..** crashes because of memory corruption. The configuration is as show below:

```
kron occurrence Daily-writeNet at 11:50 recurring
  policy-list writeNet
!
kron occurrence Daily-showtech at 13:50 recurring
  policy-list showtech
!
kron policy-list showtech
  cli show tech-support password | redirect tftp://194.25.4.197/tech/ms1-ag9!
kron policy-list writeNet
  cli copy running-config rcp://c@194.25.4.197/ms1-ag9
!
```

The **cli copy running-config rcp://c@194.25.4.197/ms1-ag9** command works, but the **cli show tech-support password | redirect tftp://194.25.4.197/tech/ms1-ag9** command crashes.

There is no workaround.

- **CSCto97888** (Catalyst Switches 3750-X and 3560-X)

  GLC-BX-D/U, CWDM, DWDM SFP inserted in ports 2 or 4 of the Gazerbeam 10G uplink module LEDs do not light up and it shows 'notconnect' even though port is physically connected.

- **CSCt33952**

  When rsh command constructs are used within Tclscript, Tcl fails to send the router hostname which causes the rsh command constructs to fail authorization to a remote router.

  There is no workaround.

- **CSCt34693**

  An EEM script that executes on a syslog event causes the Cisco router to fail with the following error message.

  000199: *Aug 23 16:49:32 GMT: %BGP-5-ADJCHANGE: neighbor x.x.x.x Up

  Exception to IOS Thread:

  Frame pointer 0x30CF1428, PC = 0x148FDF84

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog

  -Traceback=

  

  There is no workaround.

- **CSCt387275**

  When running the command **show snmp engineID** on a switch with WS-X45-SUP7-E running cat4500e-universalk9.SPA.03.01.00.SG.150-1.XO.bin, it shows same engineID 800000090300000000000000 from different switches. It seems that the switch has picked up interface Fa1 macaddress as its engineID.
The output is as shown below:

```
#show snmp engineID
Local SNMP engineID: 800000090300000000000000
#show int f1
FastEthernet1 is down, line protocol is down
Hardware is RP management port, address is 0000.0000.0000 (bia 0000.0000.0000)
```

The workaround is to manually configure snmp engineID from cli.

- **CSCuh03176**

  The Privilege commands are not appearing in the configuration of a Catalyst switch.

  When you enter the `privilege interface level 3 switchport port-security mac-address sticky` command and save the configuration, the command is not visible in neither the startup configuration nor the running configuration. However, privilege level 3 users can view the command and can use it. If you reload the switch, the command is still is not visible in the configuration and also becomes unavailable to the privilege level 3 users.

  The workaround is to use the `aaa authorization` global configuration command to access the commands available for a particular user from the AAA server.

- **CSCui75238**

  A Cisco Catalyst 3750X switch experiences a memory leak when trying use applications like `webauth`, `web_exec` and so on over secure communication (https).

  The workaround is to disable https (secure communication) and use http for HTTP requests.

- **CSCum22694**

  On the Cisco enhanced EtherSwitch service module (SM-ES2-24P), running the `logging source-interface #` command, does not set the source interface for syslog messages sent to a syslog server.

  There is no workaround.

- **CSCum75450**

  In a Catalyst 3750X switch stack, the switches experience a slow performance with the following message. Sometimes the switch stops responding and is not recovered until power cycling.

  ```
  %SUPQ-4-CPUHB_RECVASTARVE: Still seeing receive queue stuck after throttling
  ```

  You may also observe the following messages when the problem occurs.

  ```
  %PLATFORM_RPC-3-MSG_THROTTLED: RPC Msg Dropped by throttle mechanism
  %XDR-6-XDRIPCNOTIFY: Message not sent to slot X because of IPC error timeout. Disabling linecard. (Expected during linecard OIR)
  ```

  The issue is observed in switches running 12.2(58)SE or later. It also includes 15.0SE releases and 15.2E releases.

  The workaround is to configure a longer logging interval. For example,
**Resolved Caveats**

**ip access-list logging interval <value>**
If the issue persists after setting a longer logging interval, you must power cycle the switch.

- **CSCum77450**
  In a switch stack consisting of Catalyst 2960S switches running 15.0(2)SE4, the MAC address tables on all the stack members are not synchronized with the master switch. This issue is observed when the number of member ports is higher than 4.
  The workaround is to configure the missing MAC addresses manually.

- **CSCun01172**
  When configuring VLANs on 3750X stacked switches, the CLI experiences a delayed or slow response.
  The workaround is to configure the VTP domain name with VTP enabled.

- **CSCun25154**
  A change in the behaviour of DHCP client is observed between 15.0(2)SE2 and 15.0(2)SE4 releases.
  There is no workaround.

- **CSCun26893**
  On a stack of four WS-C3750X-48PF-S switches running IOS "c3750e-universalk9-mz.150-2.SE5.bin", the CPU Utilization is 99%, majorly due to the process "ASP Process Crea". The output is as shown:

```plaintext
b-la1-013-sw-01#sho proc cpu sort
CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 84%
--More-- PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
 PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
 363  99416 3304  30089 50.39% 43.54% 22.12%   0 ASP Process Crea
 10  843481803 98980536       8521 18.55% 18.03% 18.08%   0 Hulc LED Process
```

When trying to remove the macros by running the command "no macro auto global processing", the CPU comes back to normal but the master switch crashes.

The workaround is to reload the stack. The CPU remains low for a while. Removing the macros at this time does not cause the master switch to crash.

- **CSCun34745**
  After system reload, `ip ssh source-interface` shows in startup-config but disappears from running-config. This is seen in both the scenarios as mentioned below.

  **<Scenario 1>**
  1. Configure `ip ssh source-interface <interface>` CLI
     ```plaintext
     (config)#ip ssh source-interface gi0/3
     ```
  2. In `show run` output, it will show `ip ssh source-interface <interface>` CLI
  3. Configure same <interface> (which is configured in `ip ssh source-interface` CLI) from switch-port to routed-port.
     ```plaintext
     (config)#interface gi0/3
     (config-if)#no switchport
     ```
4. Step 4: In show run output, it will not show `ip ssh source-interface <interface>` CLI

**<Scenario 2>**

1. Configure some `<interface>` from switch-port to routed-port.

   ```
   (config)#interface gi0/3
   (config-if)#no switchport
   ```

2. Configure “`ip ssh source-interface <interface>`” CLI with same interface mentioned in step 1 i.e. `(config)#ip ssh source-interface gi0/3`

3. In show run output, it will show “`ip ssh source-interface <interface>`” CLI configured

4. Save the configuration and reload

5. After reload, in show run output, it will not show “`ip ssh source-interface <interface>`” CLI

The workaround is to re-configure `ip ssh source-interface <interface>` CLI.

- **CSCun64258**

  When around 500 Vlans are configured on a switch running IOS 15.0(2)SE5, and then if the interface is moved down or up, the switch shows high CPU Utilization, with maximum usage by 802.1x switch process for 3 minutes.

  The issue is not seen on switches running IOS 15.0(2)SE4

  The workaround is to disable the device sensor as `no macro auto monitor`.

- **CSCun70144** (Catalyst Switches 3750-X and 3560-X)

  When 802.1x authentication is running on the port along with ip device tracking, there is a memory leak bug in epm code resulting in depletion if IDs and tracebacks similar to this:

  ```
  -Traceback= 4FCA14z 51FAFCz 14B902Cz 14BA198z 14BA4A8z 14BAA28z 14BABB34z 146AB94z 264DB98z 264EA0Cz 264EC00z 26BF904z 26BA058z
  Mar 10 04:14:24.140 CET: %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)
  ```

  When running `show epm session sum`, it shows one session cloned multiple times, for example:

  ```
  GigabitEthernet0/9 10.1.10.108 0050.56ac.0930 10 0000-0000-0000-0000-0000
  GigabitEthernet0/9 10.1.10.108 0050.56ac.0930 10 0000-0000-0000-0000-0000
  ```

  Then the number of cloned sessions increases with the time.

  This issue is seen on stacked 3650X and stacked 3750X switches, running IOS 15.0.2-SE5 and 15.2.1E1.

  There is no workaround.

- **CSCun80959**

  Designated port on the Root Bridge experiences a block forward for 30 seconds. This issue occurs because the message-time (the period of time a packet is alive in the network) is almost equal to max-age (the period of time a packet is allowed to stay in the network). When message-time >= max-age, the switch receives an agedMsg on the forwarding port which moves the port to a blocking state.

  There is no workaround.

- **CSCun83858**
The lightweight wireless access point macro applied to an interface which has both CDP and LLDP enabled flaps continuously. The CDP neighbor devices are discovered initially on the Gi0 interface of the AP and then after a few seconds, the neighbour devices are discovered on the main interface and the sub-interface (Gi0 and Gi0.1) of the AP. After some time, CDP neighborship times out for the Gi0 interface and the macro configuration for $LINKUP == "NO" event is applied on the switch interface.

The workaround is to disable LLDP on the switch interface.

- CSCuo17293
  When port-security is configured on all ports and when the end host is moved, the mac address table is out of sync.
  The workaround is to clear the mac address table.

- CSCuo50456 (Catalyst Switch WS-C3560X)
  When Resilient Ethernet Protocol (REP) is running, CPU usage is high during a failover.
  There is no workaround.

- CSCuo59926 (Catalyst Switches 3750-X and 3560-X)
  Cisco TrustSec crashes while assigning new Source Security Tags (SGTs) and then applying the corresponding Role-Based Access Control Lists (RBACLs).
  The workaround is to limit the number of RBACL entries.

- CSCuo92394
  When a PC with 802.1x capability is connected to the IP phone, and the PC boots up, the IP Phone sends CDP port UP to the switch, which restarts 802.1x authentication process. The Switch deletes running 802.1x authentication process and starts over upon receiving CDP port UP from the IP phone. It makes authentication process fail on the machines which can only complete it in first run.
  There is no workaround.

- CSCuo97298
  On Cisco IOS Release 15.0(2)SE6, the PS-FAN falls to FAUTY status after upgrading the IOS software from Cisco IOS Release 15.0(2)SE5. The show env stack command displays the following output:

  SWITCH: 1
  FAN 1 is OK
  FAN 2 is OK
  PS-FAN1 is FAULTY
  PS-FAN2 is NOT PRESENT
  TEMPERATURE is OK
  Temperature Value: 35 Degree Celsius
  Temperature State: GREEN
  Yellow Threshold : 46 Degree Celsius
  Red Threshold    : 60 Degree Celsius
  POWER is OK
  RPS is NOT PRESENT
SWITCH: 2
FAN 1 is OK
FAN 2 is OK
PS-FAN1 is FAULTY
PS-FAN2 is NOT PRESENT
TEMPERATURE is OK
Temperature Value: 34 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 60 Degree Celsius
POWER is OK
RPS is NOT PRESENT

The workaround is to downgrade to Cisco IOS Release 15.0(2)SE5 or to use the latest release which has fix for this issue.

- CSCup20936 (Catalyst Switches 3750-X)
  The following syslog message should be removed or it should not be generated by default:
  May 20 04:44:33 CEST: %CTS-6-SAP_REKEY_TIMER_EXPIRED: SAP Rekey Timer Expired for interface(Te2/1/1) after 169 sec.
  The message should be removed because it is seen only if the switch being used is an initiator of a rekey. Also on high speed links the messages appears very often which affects logging buffer.
  The default rekey intervals are:
  \[
  \begin{array}{ll}
  \text{Link Speed (S)} & \text{Rekey Interval} \\
  \text{10M} < S =\text{< 100M} & 5 \text{ hours} \\
  \text{100M} < S =\text{< 1G} & 30 \text{ min} \\
  \text{5G} < S =\text{< 10G} & 3 \text{ min} \\
  S > 10G & 45 \text{ sec}
  \end{array}
  \]
  The other option would be to modify the behaviour and generate such syslog each time when a rekey happens no matter which ends initiate it.
  There is no workaround.

- CSCup49030
  With EX90/EX60 is configured to communicate over the data vlan, EX cannot get ip via DHCP over the data Vlan. This is because switch expects the packet to arrive on voice vlan from EX, but EX is sending packets on data vlan. All DHCP requests get dropped at the switch. Hence EX is not able to get the ip address.
  The workaround is to disable one of the following:
    - Port-security
    - Voice Vlan on the interface (remove voice vlan config from the interface)

- CSCup61889 (Catalyst Switches 3750-E and 3750-X)
Due to a timing issue, the port channel member port on the slave switch of the stack loops during boot up. The issue occurs only on the member port that is configured as the first port in a cross-stack EtherChannel configuration and when Nexus devices are connected to Cisco devices. Due to Link Aggregation Control Protocol (LACP) graceful convergence, when both the devices are up and in sync (S) state, Cisco devices start transmitting even before the devices get onto collecting (C) state. This causes the port to be pulled down by the Nexus devices. When this happens during boot up, the EtherChannel hardware programming for the port is cleared even when the port is bundled in the port-channel.

The workaround is to enter the `shutdown/no shutdown` command on the port-channel interface or disable `lacp graceful-convergence` on the port-channel on peer devices.

- **CSCuq06262** (Catalyst Switches 3750-E and 3750-X)
  When a switch stack is configured in VTP client mode with VTP password, the show command for the stack master displays the VTP operating mode as client, whereas the member switches display the VTP operating mode as server.
  The workaround is to remove the VTP password.

- **CSCuq49531**
  10G link convergence is better than 1G convergence during link pull or link down. When the interface is lost in a port channel the flow switch over to the backup link is faster for 10G uplink when compared to a 1G uplink. This is because interface state polling is faster for 10G uplink than 1G uplink.
  There is no workaround.

### Caveats Resolved in Cisco IOS Release 15.0(2)SE6

Unless otherwise noted, these caveats apply to Catalyst 3750-X, 3750-E, 3560-X, and 3560-E switches

- **CSCI44340**
  On stack switches, the first switch is configured as client and the other switch is configured as DHCP server and TFTP server. When you reload the first switch, the auto configuration does not start.
  There is no workaround.

- **CSCto13462**
  In a network that consists of two DHCP clients with same client id and different mac addresses, the DHCP server reloads when one of the clients releases its DHCP address.
  There is no workaround.

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

- **CSCts43759**
  The CPU usage increases when you configure the local proxy Address Resolution Protocol (ARP) feature on a Switch Virtual Interface (SVI).
  The workaround is after you configure the SVI, remove the local proxy ARP configuration by entering the `no ip local-proxy-arp` command, and reconfigure it by entering the `ip local-proxy-arp` command.

- **CSCts80209**
A switch configured with login quiet-mode resets when you enter the `login block-for` or `no login block-for` commands.

There is no workaround. Nevertheless, to avoid a reset, do not enter the `login block` or `no login block-for` commands.
• CSCtz14399

The TCP stack of Cisco IOS Software impose a vulnerability caused by terminating the TCP connections incorrectly. This vulnerability can be exploited by allowing an unauthenticated, remote attacker to send a crafted sequence of TCP ACK and FIN packets to an affected device thereby causing an ACK storm which results in excessive network utilization and high CPU usage.

The workaround is to use the `clear tcp tcb 0x<tcb_num>`, where the hexadecimal value is the address of the TCB with a connection state of LASTACK in `show tcp brief` command.

• CSCua69378

When you configure Flex Link on stacks containing interfaces from different switches, the interfaces start flapping continuously.

The workaround is to remove the Flex Link configuration from the interfaces.

• 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.

• CSCue11350 (Catalyst Switches 3750-X and 3560-X)

When the traffic rate on a CTS-enabled interface connecting Catalyst C3750X switch and Integrated Services Router (ISR) is higher than 950 Mbps, the interface wedges and blocks all the traffic.

The workaround is to reload the switch and reduce the traffic rate to less than 950 Mbps.

• CSCue95644

When you upgrade a device to a Cisco IOS or Cisco IOS XE release that supports Type 4 passwords, enable secret passwords are stored using a Type 4 hash which can be more easily compromised than a Type 5 password.

The workaround is to configure `enable secret` command on an IOS device without Type 4 support, copy the resulting Type 5 password, and paste it into the appropriate command on the upgraded IOS device.

• CSCue97722 (Catalyst Switches 3750-X and 3560-X)

In a stack of Catalyst 3750x switches, port security enabled ports block all the network traffic through them. Using the `sh mac address-table` command shows that the mac address is learned as static on the master switch, whereas the member switches do not have this mac address on their mac address table.

There is no workaround.

• CSCug29687

Memory leak occurs when you map the Entity MIB API, and configure clustering on the switch. The workaround is to perform any one of the following steps:

- Remove the clustering configuration from the switch.
- Reload the switch to release the memory occupied by the Entity MIB API process.

• CSCug47095

During the SNMP walk, the `vlanTrunkPortDynamicStatus` object in the CISCO-VTP-MIB module shows “notTrunking(2)” for the members of Port-channel trunk ports.

The workaround is to use the CLI to get the correct values.
- CSCug89494 (Catalyst Switches 3750-X and 3560-X)
  Memory leak occurs when the `show macsec interface` command is entered on the inactive Wall-E interfaces.
  The workaround is to not to enter the `show macsec interface` command on the inactive Wall-E interfaces.
- CSCug90127 (Catalyst Switches 3750-X and 3560-X)
  The switch port goes in to the err-disabled state due to port security violations.
  The workaround is to run the `no switchport` command on the interface.
- CSCuh45966
  Device under test (DUT) fails with traceback when you enter the `configure replace target-url` command. The issue occurs when the following message is forwarded to `forwardFormattedMessage_to_logger()` API.
  ```
  % eula should be accepted for non-interactive management for license-level = ipservices (stack3-1-31-1-2)
  ```
  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, the connection over 802.3at POE+ fails.
  The workaround is to move all the affected POE+ devices to the stack master.
- CSCui07884 (Catalyst Switches 3750-X and 3560-E)
  The stacked switch setup fails when you change or remove an existing password while the relayed console waits for the authentication prompt.
  The workaround is to reduce the number of changes to the password in the console or VTY when the relayed console waits for the authentication prompt.
- CSCui20519 (Catalyst Switches 3750-X and 3560-E)
  In a Cisco Catalyst Switch stack of 8 member switches, a memory leak is observed in the HRPC pm request handler process. The issue occurs after reloading the stack members or after online insertion and removal (OIR) of the transceivers that are DOM capable.
  There is no workaround.
- CSCui21748 (Catalyst Switches 3750-X and 3560-E)
  The I2C failure occurs when reading the payload from Microcontroller Unit (MCU) to CPU and writing the payload from CPU to MCU. During the I2C read and write operations, CPU and MCU go out-of-sync and the communication between them stops, and the CPU declares that the FRONT-END is inactive.
  There is no workaround.
- CSCui33479 (Catalyst Switches 3750-X and 3560-X)
  The `sh env fan` command does not detect faulty power supply fans on a switch.
  There is no workaround.
• CSCui52743
  When you enable the Address Resolution Protocol (ARP) retry feature on the switch, the CPU usage increases.
  There is no workaround.
• CSCui56736 (Catalyst Switches 3750-X and 3750-E)
  When VLAN Trunk Protocol (VTP) version 3 is configured on stacked switches, the inconsistency in VTP mode is observed between the master switch and the member switch. When you run the `show vtp status` command, the master switch shows the status as Server for VLAN and Transparent for Multiple Spanning Tree (MST), and the member switch shows the status as Primary Server for both VLAN and MST.
  The workaround is to configure the switch to VTP version 2 and then reconfigure the switch to VTP version 3.
• CSCui59769 (Catalyst Switches 3750-X and 3750-E)
  The Web Cache Communication Protocol (WCCP) traffic drops when you reload the master switch with the stack switch.
  There is no workaround.
• CSCuj36089
  In a topology in which a Catalyst 3750X switch acts as the multicast router, a receiver constantly sends join messages to a multicast group (*,G) before the source starts sending the multicast traffic. When the source starts sending traffic to the multicast group, an (S,G) is created and some of the initial packets sent by the source are lost. Once the (S,G) is programmed for the traffic sent by the source, all the subsequent multicast traffic reaches the receiver.
  There is no workaround.
• CSCuj48700
  A switch reboots unexpectedly while using dot1x authentication with IP Device Tracking (IPDT) enabled. If `ip device tracking probe {delay delay}` is configured and the switch is operating near the maximum IPDT limit of 2048 hosts, there is a probability that a host may have its delay timer started, but released before it expires.
  Use one of the following workarounds:
  – Keep the number of hosts less than 2048.
  – Turn off probe delay.
  – Disable dot1x authentication, which in turn disables IP HOST TRACK process.
• CSCuj65057 (Catalyst Switches 3750-X and 3750-E)
  When you configure per-VRF on a AAA TACACS+ server group, the `ip vrf forwarding` command does not appear in the running configuration after reloading the stack master. This issue takes place only in stack configurations.
  The workaround is to use `vrf definition` command instead of `ip vrf` command to configure per-VRF.
• CSCuj77426 (Catalyst Switch 3750-E)
  After performing a `shut` or `no shut` on the ports of a Catalyst Switch, the status of some of the ports are displayed as Not Connected, even if they are connected to a remote device.
  The workaround is to perform a `shut` or `no shut` on the affected ports.
Resolved Caveats

- **CSCuj77254**
  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.

- **CSCuj98188** (Catalyst Switches 3750-X and 3560-X)
  Memory leak occurs in the Service Module (SM) when handling the HRPC message.
  There is no workaround.

- **CSCul02715**
  The switch reboots if the shutdown and no shutdown commands are repeatedly entered for the alternating ports in an 8-node Resilient Ethernet Protocol (REP) ring segment. The following error message is displayed:
  Debug Exception (Could be NULL pointer dereference) Exception (0x2000)
  There is no workaround.

- **CSCul06810**
  On a switch stack, when Resilient Ethernet Protocol (REP) and Open Shortest Path First (OSPF) are configured, the OSPF fails at Exstart during the master switch-over.
  The workaround is to bounce the forwarding REP port on the switch stack.

- **CSCul17159**
  In response to an NTP control request, the offset value in the reply packet received from a Catalyst 3560X/E switch running on 12.2(58)SE or later is different from the offset value in a packet received from a switch running on 12.2(55)SE or earlier.
  The workaround is to downgrade the switch to 12.2(55)SE or earlier.

- **CSCul17852**
  When you repeatedly run the shut and no shut command in the alternating ports on a 8 node REP ring, the stack member with REP secondary edge port drops the multicast traffic for 20 to 50 seconds.
  There is no workaround.

- **CSCul48789**
  The Webauth leak occurs during the Webauth authentication process, and the Enterprise Policy Management (EPM) leak occurs when authentication policies are applied through EPM.
  There is no workaround.

- **CSCul55991**
  When IPV6 MLD Snooping is enabled on a switch and the switch is restarted, the packets that are destined to Solicited-Node multicast address are not forwarded in some rare instances.
  The workaround is to disable the IPv6 MLD Snooping, and then enable the IPv6 MLD Snooping.

- **CSCum56403**
  When you apply ACL to an interface or an VLAN and if there is a shortage of Ternary Content-Addressable Memory (TCAM), the Flow-Based Switch Port Analyzer (FSPAN) does not work as expected when reloading the FSPAN session.
  The workaround is to reconfigure the VLAN -based FSPAN session.
Resolved Caveats

CSCum78626 (Catalyst Switches 3750-X and 3750-E)
When a new switch is added to the stack, and if the stack has the Hot Standby Router Protocol (HSRP) configured, the newly added member switch fails.
There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE5

- CSCto33458 (Catalyst Switches 3750-X and 3560-X)
  After continuously sending 1000 packets/second on C3KX-SM-10G service module's 10G interface for more than 1 hour, the C3KX-SM-10G service module could go down and all the Netflow flow records cannot be created.
  There is no workaround.

- CSCty66702
  In Policy Based Routing (PBR), if the first match clause is removed, the packets are forwarded to the next hop IP address of the second match clause. This feature, which previously showed errors, is now functioning properly.
  There is no workaround needed.

- CSCua74302 (Catalyst Switches 3750-X and 3560-X)
  (LAN Base) ACLs applied to outbound traffic on the switch virtual interface (SVI) do not work.
  There is no workaround.

- CSCud89149 (Catalyst Switch 3750-X)
  On a switch stack, IPDT (Cisco IP Telephony Design) on the master switch does not update a new VLAN ID after authentication with 802.1x is successful. As a result, connectivity is not possible even though the client machine has a valid IP address, and dACLs (downloadable ACLs) are not applied on the interface.
  The workaround is to configure authentication as open so that traffic is allowed only after authentication is successful. Alternatively, add a short lease DHCP server on the default access VLAN so that clients are assigned different IP addresses on the default access VLAN and dynamic VLAN.

- CSCue49529 (Catalyst Switches 3750-X and 3750-E)
  If a Catalyst 3750-X switch stack that runs Cisco IOS Release 15.0(2)SE1 is connected to a Catalyst Switch 2960 using cross-stack etherchannel, and if the master switch is power cycled, the line protocol of the member interfaces and channels flap. If the channel goes down, there is no message output displayed on the stack switch.
  There is no workaround.

- CSCuf48025 (Catalyst Switch 3750-E)
  Netflow cache is not created after applying a flow monitor to the interface on the member switch.
  There is no workaround.

- CSCuf26848
  CPU usage goes above 90% when Internet Group Management Protocol (IGMP) version 3 report packets are sent to the switch which has IGMP version 2 configured on the switch virtual interface.
  The workaround is to either disable multicast fast convergence or configure IGMP version 3 on switch virtual interface.
Resolved Caveats

- CSCug52714
  TACACS+ single connect authentication request from a switch stack takes around 10 to 12 minutes to failover to secondary server after the primary TACACS server is unreachable.
  The workaround is to disable TACACS+ single connect configuration on the switch.

- CSCuh97014 (Catalyst 3750-X and 3560-X switches)
  When the master switch in a switch stack is reloaded, the Cisco TrustSec (CTS) link configured on the CK3X-SM-10G port of the member switch goes down.
  The workaround is to enter a `shutdown` command followed by the `no shutdown` command on the ports of the service module.

- CSCui24166
  On configuring Cisco TrustSec (CTS) in manual mode with the `no switchport` command, the CTS link does not come up if the link is on member switch.
  The workaround is to enter a `shutdown` command followed by the `no shutdown` command on the port.

- CSCui41032
  Switch runs out of memory within few seconds of configuring the `level <n> show spanning-tree active/detail` privilege EXEC command.
  There is no workaround.

- CSCui44104 (Catalyst 3750-X and 3560-X switches)
  On configuring Cisco TrustSec (CTS) on LACP port-channel of the switch, where the peer port-channel is any switch other than a Catalyst 3750-X or 3560-X, the port-channel goes to suspend state.
  There is no workaround.

- CSCui87793
  Web authentication does not work.
  There is no workaround.

- CSCui90464 (Catalyst Switches 3750-X and 3560-X)
  MACsec link traffic drops periodically.
  There is no workaround.

- CSCuj81084 (Catalyst Switches 3750-X, 3560-X and 3560-E)
  In a switch stack where EnergyWise is enabled, memory leak is observed when the `show energy wise children` privileged EXEC command is entered or when the `cewEntEnergyUsage` object ID is polled.
  The workaround is to disable EnergyWise.

Caveats Resolved in Cisco IOS Release 15.0(2)SE4

- CSCug24114
  CTS environment-data download failed on non-seed device after reboot.
  The workaround is to remove the Protected Access Credential (PAC) encryption key (`no pac key` RADIUS server configuration command) and then configure the key again (`pac key` command).
Resolved Caveats

- **CSCug62154**
  When the switch is started using TACACS+ configurations, the CPU utilization increases to 100% and the VTY device does not work.
  The workaround is to remove the TACACS+ configurations and restart the switch.

- **CSCuh41077**
  The ipAddrEntry value in the IP Address Table shows an interface index that is not exposed by the ifEntry Object ID.
  There is no workaround.

- **CSCuf77683**
  Internal VLANs are displayed when the `show snmp mib ifmib ifindex` command is entered or the SNMP is queried for the ipMIB object.
  The workaround is to check if the displayed VLANs are internal and then to hide them.

Caveats Resolved in Cisco IOS Release 15.0(2)SE3

- **CSCta43825**
  CPU usage is high when an SNMP Walk of the Address Resolution Protocol (ARP) table is performed.
  The workaround is to implement SNMP view using the following commands:

  ```
  snmp-server view cutdown iso included
  snmp-server view cutdown at excluded
  snmp-server view cutdown ip.22 excluded
  snmp-server community public view cutdown ro
  snmp-server community private view cutdown rw
  ```

- **CSCts95370**
  If an ACL is configured on a router VTY line for ingress traffic, the ACL is applied for egress traffic also. As a result, egress traffic to another router on an SSH connection is blocked.
  The workaround is to permit egress traffic to the specific destination router using the `permit tcp host <destination router IP address> eq 0 any` interface configuration command.

- **CSCub45763**
  The device connected to the switch crashes when a CDP data frame is processed. The `SYS-2-FREEFREE` and `SYS-6-MTRACE` messages are displayed.
  The workaround is to disable CDP using the `no cdp run` global configuration command. This workaround is not applicable if the connected device relies on or supports a phone or voice network.

- **CSCub85948**
  Memory leak is seen in the switch when it sends CDP, LLDP or DHCP traffic and when the link flaps.
  The workaround is to apply protocol filters to the device sensor output by entering the following global configuration commands:
Resolved Caveats

no macro auto monitor
device-sensor filter-spec dhcp exclude all
device-sensor filter-spec lldp exclude all
device-sensor filter-spec cdp exclude all

If the memory leak continues in the "DHCPD Receive" process, disable the built-in DHCP server by entering the no service dhcp global configuration command.

- CSCuc10143
  Spurious traps observed periodically on removal of power to RPS.
  There is no workaround.

- CSCuc40634
  STP loop occurs on Flexstack connected by parallel links when a link state is changed on Flexlink port.
  The workaround is to change the switch to root bridge.

- CSCuc41395
  Policy Based Routing (PBR) entry on the switch does not become inactive even after the PBR route's next hop is lost. The traffic continues to take failed PBR path instead of the next available best path.
  There is no workaround.

- CSCuc90103 (Catalyst 3750-X and 3560-X switches)
  On running show interface command, incorrect value is displayed in input error counter.
  There is no workaround.

- CSCuc95754
  PortASIC's TCAM test fails when you execute on-demand diagnostics through diagnostics start command.
  You can ignore the results of on-demand diagnostics if POST succeeds on boot up.

- CSCud96215 (Catalyst 3560-E and 3750-E switches)
  LSG Downlink port flaps when SFP+ is used as an uplink port. This issue also appears if SFP+ is configured in a flexlink configuration.
  There is no workaround. The configuration recovers automatically.

- CSCud44884
  If a policy map attached to the switch interface is modified then the corresponding QoS policy works incorrectly.
  The workaround is to delete the policy map, create a new policy map and then attach it to the interface.

- CSCud76611
  The switch blackholes traffic redirected by Web Cache Communication Protocol (WCCP). This issue occurs when the WCCP cache engine is shut down and the cache is not cleared.
  The workaround is to use Cisco IOS Release 12.2(55) or later.

- CSCud83248
  When native VLAN is configured on the trunk or when switchport trunk native vlan 99 is configured on the interface, spanning-tree instance is not created for native VLAN.
The workaround is to keep VLAN1 as a native on the trunk. In Cisco IOS Release 15.0(2) SE, dot1x is enabled by default and causes authentication fail in the native VLAN. This results in pm_vp_statemachine not triggering any event to spanning tree. To disable dot1x internally, run the no macro auto monitor command. The stp instance is created for native vlan 99 after running the show and no show command on the interface.

- CSCue34250
  The Web Cache Communication Protocol (WCCP) traffics are not redirected after reloading the switch.
  The workaround is to remove the WCCP redirects command from the interface and then add them back on the interface.

- CSCue86180
  On the Catalyst 2960S switch stack, when the login block command is configured and the running config is saved using the wr command on the master, it makes the master down. When the running config is saved on the new master, the following lines are displayed on entering the show running-config command.

```
ip access-list extended sl_def_acl
  deny tcp any any eq telnet
  deny tcp any any eq www
  deny tcp any any eq 22
  permit ip any any
```
  There is no workaround.

- CSCue87815
  When the secret password is configured, the password is not saved. The default password is used as the secret password.
  The workaround is to use the default password to login and then change the password.

- CSCue92286 (Catalyst 3750-X switches)
  A vulnerability in the Service Module could allow an authenticated, local attacker to gain root access to the kernel running on the Service Module. The attacker can use the default credentials to log on to the Service Module and take complete control of the operating system running on the Service Module.
  There is no workaround.

- CSCue92705 (Catalyst 3750-E and 3560-E switches)
  The device sensor related memory leak is still visible in DHCPD Receive, CDP Protocol, and Net Background processes even after disabling the device sensor feature by entering the no macro auto monitor command. This symptom is observed in Cisco IOS 15.0(2)SE1 Release, 2960S, dhcp, cdp traffic, and link flapping.
  The known workaround is to enter the no service dhcp command if the switch is not a DHCP server and configure the device sensor as follows:

```
device-sensor filter-spec cdp exclude all
device-sensor filter-spec dhcp exclude all
device-sensor filter-spec lldp exclude all
```

- CSCue64945 (Catalyst 3750-X and 3560-X switches)
In the module with 1Gb/10s SFPs interface, the traffic from the active port gets dropped when MACsec is configured on the inactive interface and the switch or module is reloaded.

The workaround is to perform any of the following action:

- Enter the `macsec` command on the active interface always and not on the inactive interface.
- Enter the `no macsec` command on the inactive 10-Gigabit link and then reload the switch or reload the wall-emodule (frulink reload).
- Enter the `macsec` and `no macsec` commands on the active interface to restore the traffic

- CSCug89494 (Catalyst 3750-X and 3560-X switches)
  Small memory leak occurs:
  - When a one Gigabit SFP is connected to the port and the `show macsec int` command is entered on the ten Gigabit interface.
  - When a ten Gigabit SFP is connected to the port and the `show macsec int` command is entered on the one Gigabit interface.
  - When `show macsec int` command is executed on a inactive/operationally down interface.

  There is no workaround. The suggestion is to make less use of the `show macsec int` command on the interfaces when SFP is not present.

- CSCuf80350 (Catalyst 3750-X switch)
  When reloading a switch in a stack that contains a service module inside a member switch, the links on the service module does not show up after reloading the member switch.

  The known workaround is to restore the link by entering shut and no shut commands on the ports in the service module.

---

**Caveats Resolved in Cisco IOS Release 15.0(2)SE2**

- CSCtg15739
  When a client fails to authenticate in the multi-auth mode, the session continues to be active indefinitely.

  The workaround is to enter the `clear authentication sessions` privileged EXEC command to clear information for all authentication manager sessions.

- CSCty63718
  The `down-when-looped` interface configuration command is not supported with default speed or with 1000BaseT advertisements on the gigabit medium independent interface (GMII interface). This is because the down-when-looped feature and 1000BaseT advertisements both make use of the "next page" function as defined in IEEE 802.3, clause 28 and may result in the link staying down.

  There is no workaround.

- CSCue19317 (Catalyst Switches 3560-X and 3750-X)
  If the switch is upgraded from Cisco IOS Release 15.0(2)SE or 15.0(2)SE1 by using the `archive download-sw /allow-feature-upgrade /upgrade-ucode <tar Image>` command, the ucode upgrade is performed twice, once at the time of archive download and another at IOS boot up. This delays the switch boot time. This behavior is also seen when using the `force-ucode-reload` option.

  There is no known workaround.

- CSCud01798 (Catalyst Switches 3560-X and 3750-X)
The following message is seen intermittently:

**FRU Power Supply is not responding**

There is no workaround. This message does not indicate a hardware failure of any kind.

### Caveats Resolved in Cisco IOS Release 15.0(2)SE1

- **CSCee32792**
  - When using SNMP v3, the switch unexpectedly reloads when it encounters the `snmp_free_variable_element`.
  - There is no workaround.

- **CSCtg39957**
  - Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate this vulnerability.
  - This advisory is available at the following link:
    

**Note**
The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:


- **CSCtg47129**
  - The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.
  - Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.
  - This advisory is available at the following link:
    

**Note**
The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.
Resolved Caveats

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

- CSCth03648
  When two traps are generated by two separate processes, the switch fails if one process is suspended while the other process updates variables used by the first process.
  The workaround is to disable all SNMP traps.

- CSCth59458
  If a redundant power supply (RSP) switchover occurs during a bulk configuration synchronization, some of the line configurations might disappear.
  The workaround is to reapply the line configurations.

- CSCti95154
  Beginning with Cisco IOS Release 12.2(52)SE, the device tracking table could map only one IP address to a single MAC address. This restriction has been removed, and several IP addresses can now be mapped to a single MAC address.

- CSCti12389
  The `show ip dhcp pool` command displays a large number of leased addresses.
  The workaround is to turn off `ip dhcp remember` and reload the switch.

- CSCti64716
  The following warning messages might be displayed during the boot process even when a RADIUS or a TACACS server have been defined:
  
  ```
  %RADIUS-4-NOSERVNAME:
  or
  %AAAA-4-NOSERVER: Warning: Server TACACS2 is not defined
  ```
  
  There is no workaround.

- CSCtt37757
  The secure copy feature (copy: source-filename scp: destination-filename command) does not work.
  There is no workaround.

- CSCtt14788 (Catalyst 3560-X and 3750-X switches)
  NetFlow Data Export (NDE) packets might be dropped when virtual routing and forwarding (VRF) is configured on the switch and the exported traffic has conflicting information from the VRF tables and the routing information base.
  There is no workaround.

- CSCtt33903
  This problem occurs when the Enterprise Policy Manager (EPM) for a device connected to an interface is authorized in closed mode and no policies are configured or downloaded. If no port ACL is configured, the auth-default access control list (ACL) is applied to the switch. If another device is connected to this device, restricted VLAN (authentication event interface configuration command) is enabled on the port. The Application Control Engine (ACE) is not configured to permit traffic originating from the connected device, and IP packets are dropped.
The workaround is to configure a port ACL to allow IP traffic for the specific IP range for the connected devices on the interface.

- CSCtx69656
  If a Catalyst 2960 switch boots with Cisco IOS Release 12.2(50)SE5 or later, a Catalyst 3750 switch that is connected by a trunk port to the Catalyst 2960 switch cannot receive the Generic Attribution Registration Protocol (GARP) data packets from the Catalyst 2960 switch.
  The workaround is to perform the following actions:
  - Run the Catalyst 2960 switch on Cisco IOS Release 12.2(25)SEE or 12.2(53)SE2.
  - Clear the Address Resolution Protocol (ARP) on the connected device.
  - Enter the `switchport noneg` command to specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent to the Layer 2 interface.
  - Ping from the Catalyst 2960 switch to the connected device.
  - Use the `line-proto-delay` command to control Switch Virtual Interface (SVI) timing.

- CSCty10239 (Catalyst 3560-E and 3750-E switches)
  When ipl=5, the Catalyst 2960 switch receives the malloc failure message of 20 bytes, and traceback occurs due to interrupt level.
  There is no known workaround.

- CSCtz91389
  When the `ip rsvp snooping` command is enabled on a Layer 2 environment, the switch stops forwarding the metadata packets.
  There is no known workaround.

- CSCtz98066 (Catalyst 3750-E, 3750-X, and 3560-X switches)
  When the master switch (Switch A) is reloaded or loses power and rejoins the stack as a member switch, any traffic stream that exits Switch A is dropped because the newly joined member is not able to establish an Address Resolution Protocol (ARP) entry for the next hop router or switch.
  Debugs confirm that Switch A does not send a GARP or ARP for the next hop, though traffic continues to be sent to the switch.
  The workaround is to add a static ARP. Ping the destination from Switch A to force the ARP to respond.

- CSCtz99447
  Local web authorization and HTTP services on the switch do not respond because of a web authorization resource limitation in the system. The resource limitation is normally caused by incorrectly terminated HTTP or TCP sessions.
  These are possible workarounds and are not guaranteed to solve the problem:
  - Enter the `ip admission max-login-attempts` privileged EXEC command to increase the number of maximum login attempts allowed per user.
  - If the web authorization module is intercepting HTTP sessions from web clients in an attempt to authorize them, try using a different browser.
  - Eliminate background processes that use HTTP transport.

- CSCua38239 (Catalyst 3750-X, and 3560-X switches)
  After reconfiguring the flow monitor in the switch interface, the `show flow monitor` shows that NAM3 is active.
The workaround is to reconfigure the flow monitor in the switch interface.

- **CSCua64859**
  The CISCO_LAST_RESORT_AUTO_SMARTPORT macro is applied to any device for which there is no built-in or user-defined macro, regardless of whether the device supports CDP, Link Layer Discovery Protocol (LLDP), or DHCP. To ensure that a device is not running a discovery protocol that matches the device to a built-in or user-defined macro, the switch waits about 120 seconds before applying the CISCO_LAST_RESORT_AUTO_SMARTPORT macro. The macro is applied to devices such as PCs, laptops, and printers. You do not need to configure MAC operationally unique identifier (OUI)-based triggers and map these triggers to a macro for these devices.

- **CSCub55790**
  The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. Affected devices that are configured as Smart Install clients are vulnerable. Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.

  This advisory is available at the following link:

- **CSCuc25654** (Catalyst 3560-X, 3750-X, and 3750-E switches)
  The SAP preshared key configured for Cisco TrustSec manual mode is saved and displayed in the configuration file as clear text.
  There is no workaround.

- **CSCua54224**
  Heavy traffic load conditions may cause the loop guard protection function to be automatically activated and almost immediately deactivated. These conditions can be caused by entering the `shutdown` and `no shutdown` interface configuration commands or by interface link flaps on more than forty ports. These log messages appear:
  ```
  %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.

- **CSCua67288**
  When quality of service (QoS) is disabled on the switch, fragmented IP packets that are sent to the switch are queued in the wrong egress queue (Queue 1). This situation causes a high number of output drops since the default buffers for Queue 1 do not have the capacity to handle data traffic.

  The workaround is to enable QoS and modify queue buffers.

- **CSCua87594**
  When a peer switch sends inferior Bridge Protocol Data Units (BPDUs) on the blocking port of the Cisco switch (with the proposal bit ON), the Cisco switch waits for three such BPDUs before responding with a better BPDU. This leads to a convergence time of more than 5 seconds. The problem appears under these conditions:

  - The Cisco switch is not configured as the root switch.
  - The Cisco switch uses Multiple Spanning-Tree Protocol (MSTP) and the peer switch uses Rapid Spanning Tree Protocol (RSTP) or rapid per-VLAN spanning-tree plus (rapid PVST+).
There is no workaround.

- CSCub14238
  With switches running Cisco IOS Release 15.0(2)SE, there was a problem when port-based address allocation was configured. The DHCP client did not receive IP addresses from the server if the client ID was configured as an ASCII string or if the subscriber ID was used as the client ID.
  This problem has been fixed now. No action is required.

- CSCub14641
  When you configure and save the monitor session source interface, the configuration is not saved after reboot.
  There is no workaround.

- CSCub24886 (Catalyst 3750-E and 3750-X switches)
  A bidirectional port on a stack member returns an incorrect status.
  There is no workaround.

- CSCub34645 (Catalyst 3750-X and 3560-X switches)
  The Cisco TrustSec link is down.
  The workaround is to reconfigure the Cisco TrustSec link layer security. You can do this in the 802.1x mode by using the cts dot1x interface configuration command or in the manual mode by using the cts manual interface configuration command.

- CSCub43035 (Catalyst 3750-X switches)
  When traffic is routed between two VLANS, multicast packets on the switch are lost for a few seconds. This happens only when the multicast source routes traffic to a group that already has a receiver on it.
  There is no workaround.

- CSCub73854 (Catalyst 3750-X switches)
  When you configure FlexLinks on the service modules and you plug the link into the port, the following syslog error message appears repeatedly:

  %SYS-3-INTPRINT: Illegal printing attempt from interrupt level. -Process= "<interrupt level>", ipl= 4, pid= 57 -Traceback= 4F0C38z 1B6CC24z 1B6B494z 2239740z 223DF24z 2258560z 2243C98z 2244188z 2286DB4z 219345Cz 2193404z 2198E44z 2198EE0z 219350Cz 219252Cz

  There is no workaround.

- CSCub93357
  If an interface is configured with the switchport port-security maximum 1 vlan command, the following error message is displayed:

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

  There is no workaround.

- CSCuc03555
  The flash memory is corrupted when you format the flash manually.
  The workaround is to reload the switch. (Note that this will erase the flash memory, and you will need to reload the software image using TFTP, a USB drive, or a serial cable.

- CSCuc17720
If the Performance Monitor cache is displayed (using the `show performance monitor cache` command) and you attempt to stop the command output display by entering the `q` keyword, there is an unusually long delay before the output is stopped.

The workaround is to enter the `term len 0` privileged EXEC command so that all command outputs are displayed without any breaks.

- **CSCub63066** (Catalyst 3560-E, 3750-E, 3560-X, and 3750-X switches)
  There is a memory loss when routing entries are updated in the table, because the switch is not releasing previously allocated memory when system resource allocation fails.
  There is no workaround.

- **CSCua12396**
  After a master switchover on a switch stack, IPv6 multicast routing fails.
  The workaround is to avoid configuring IPv6 multicast routing on larger stacks. We recommend enabling IPv6 multicast routing on stacks with five or fewer members.

## Caveats Resolved in Cisco IOS Release 15.0(2)SE

- **CSCtl48226**
  When the `show epm session summary` or `show epm` command is entered from an SSH or telnet session and another command is entered from the console, the switch might unexpectedly reset and generate crash information.
  The workaround is to enter both commands from the same session, either SSH/telnet or console.

- **CSCtl60151**
  The switch might occasionally reload after experiencing a CPU overload, regardless of what process is overloading the CPU.
  There is no workaround.

- **CSCtm11683** (Catalyst 3560-X and 3750-X)
  A Catalyst 3560-X or 3750-X switch port might stop forwarding traffic. The packet counters increment for sent packets, but not for received packets.
  The workaround, to bring up the port, is to save the configuration and to restart the switch.

- **CSCto09117**
  The switch downloads the running IOS image from the TFTP server and reboots even though the same image is currently loaded and running.
  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:

- **CSCtq38500**
When an interface is configured with the mls qos command, traffic is not matched by port-based QoS ACLs that use the range option.

The workaround is to is to configure the switch using the single port eq keyword. Alternatively, you can configure the trust under class-default setting for the same policy-map that uses the acl-range option.

- CSCqt51049 (Catalyst 3750-X and 3750-E switches)

In a switch stack, you cannot establish a console session with a member switch when an ACL is applied to the VTY lines.

The workaround is to use the following procedure when you apply an ACL to line vty 0 4 and line vty 5 15:

1. Create the vty ACL and permit the 127 network.
2. Append the vrf-also keyword to the configured access-class inbound.

See the following example:

    ip access-list standard vty-acl
        permit 127.0.0.0 0.0.0.255

    line vty 0 4
        access-class vty-acl in vrf-also
        privilege level 15
        length 0
        transport input ssh

    line vty 5 15
        access-class vty-acl in vrf-also
        privilege level 15
        transport input ssh

- CSCqt86186 (Catalyst 3750-X and 3750-E switches)

In a switch stack, the show interface command shows incorrect values for output drops.

The workaround is to use the show platform port-asic stats drops command to see the correct values.

- CSCtr07908

The archive download feature does not work if the flash contains an “update” directory. This situation is likely to occur if a previous download failed or was interrupted and the “update” directory is still left in the flash.

The workaround is to delete the “update” directory in the flash before starting the archive download.

- CSCtr19734 (Catalyst 3750-X and 3750-E switches)

A static route that has the next hop set to null0 is removed when the master switch is changed in a switch stack configuration. This situation occurs when the switch is stacked and the static route is advertised by the network 0.0.0.0 command.

The workaround is to use the ip summary-address eigrp as-number ip-address mask command to set the IP summary aggregate address for the interface through which the next hop can be found.

- CSCtr44361 (Catalyst 3750-X and 3750-E switches)

When a device is moved from one port to another in a switch stack, the SNMP data generated for the move event is incorrect.

The workaround is to ensure that the uplink to the core network is configured on the master switch (for example, a 1/0/x port).

- CSCtr55645
Resolved Caveats

OSPFv3 neighbors might flap because of the way the switch handles IPv6 traffic destined for well-known IPv6 multicast addresses.

There is no workaround.

- CSCt36715

Users connecting to the network through a device configured for web proxy authentication may experience a web authentication failure.

There is no workaround. Use the `clear tcp tcb` command to release the HTTP Proxy Server process.

- CSCtt11621

Using the `dot1x default` command on a port disables access control on the port and resets the values of the `authentication host-mode` and `authentication timer reauthenticate` commands to the default values.

The workaround is to avoid using the `dot1x default` command and set various dot1x parameters individually. You can also reconfigure the parameters that were changed after you entered the `dot1x default` command.

- CSCtt19547

The switch drops Layer 3 multicast traffic received from a Layer 2 port channel on a switch virtual interface (SVI) that is associated with a VPN Routing and Forwarding (VRF) instance.

The workaround is to flap the ingress physical interface, the SVI, or the port channel.

- CSCtt98094 (Catalyst 3750-X and 3750-E switches)

In a switch stack setup after you reload a member switch, a multilayer switching (MLS) class of service (CoS) configuration command with a specified value such as `mls qos cos 7` on the slave switch does not function anymore. This situation impacts untagged IP and Layer 2 packets.

The workaround is to ensure that when you configure a service policy on an interface, an interface default level CoS is also configured. You can use `mls trust qos cos` command in interface configuration mode.

- CSCtx33436

When using the `switchport port-security maximum 1 vlan access` command, if an IP-phone with a personal computer connected to it is connected to an access port with port security, a security violation will occur on the interface. This type of message is displayed on the console:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address XXXX.XXXX.XXXX on port FastEthernet0/1.
```

Here is a sample configuration:

```
interface gigabitethernet 3/0/47
switchport access vlan 2
switchport mode access
switchport voice vlan 3
switchport port-security maximum 2
switchport port-security maximum 1 vlan access
switchport port-security maximum 1 vlan voice
switchport port-security
```

The workaround is to remove the line `switchport port-security maximum 1 vlan access`.

- CSCtx96491
The switch does not correctly detect a loopback when the switch port on an authenticated IP phone is looped to a port configured and authenticated with dot1x security, even when `bpduguard` is configured on the interface. This situation can result in 100 percent CPU utilization and degraded switch performance.

The workaround is to configure the interface with the `authentication open` command or to configure `authentication mac-move permit` on the switch.

- **CSCty88456**

  The Catalyst 4500E series switch with Supervisor Engine 7L-E contains a denial of service (DoS) vulnerability when processing specially crafted packets that can cause a reload of the device. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:


- **CSCue23882**

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

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

**Related Documentation**

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

with complete information about the switch are available from these Cisco.com sites:

Catalyst 3750-X  

Catalyst 3560-X  

Catalyst 3750-E  

Catalyst 3560-E  

These documents provide complete information about the switches:

- `Release Notes for the Catalyst 3750-X. Catalyst 3750-E, Catalyst 3560-X, and 3560-E Switches`
- `Catalyst 3750-X and 3560-X Switch Software Configuration Guide`
- `Catalyst 3750-X and 3560-X Switch Command Reference`
- `Cisco IOS Software Installation Document`
- `Catalyst 3750-X and 3560-X Switch Getting Started Guide`
- `Catalyst 3750-X and 3560-X Switch Hardware Installation Guide`
- Regulatory Compliance and Safety Information for the Catalyst 3750-X and 3560-X Switch
- Installation Notes for the Catalyst 3750-X and 3560-X Switch Power Supply Modules
- Installation Notes for the Catalyst 3750-X and 3560-X Switch Fan Module
- Installation Notes for the Catalyst 3750-X and 3560-X Switch Network Modules
- Catalyst 3750-E and Catalyst 3560-E Switch Software Configuration Guide
- Catalyst 3750-E and Catalyst 3560-E Switch Command Reference
- Cisco Software Activation and Compatibility Document
- Catalyst 3750-E Switch Getting Started Guide
- Catalyst 3560-E Switch Getting Started Guide
- Catalyst 3750-E and Catalyst 3560-E Switch Hardware Installation Guide
- Regulatory Compliance and Safety Information for the Catalyst 3750-E and Catalyst 3560-E Switch
- Installation Notes for the Catalyst 3750-E, Catalyst 3560-E Switches, and RPS 2300 Power Supply Modules
- Installation Notes for the Catalyst 3750-E and Catalyst 3560-E Switch Fan Module
- Installation Notes for the Cisco TwinGig Converter Module
- Cisco Redundant Power System 2300 Hardware Installation Guide
- Cisco Redundant Power System 2300 Compatibility Matrix
- Cisco Redundant Power System 2200 Hardware Installation Guide
- Configuring the Cisco eXpandable Power System (XPS) 2200
- Auto Smartports Configuration Guide
- Cisco EnergyWise Configuration Guide
- Smart Install Configuration Guide
  For other information about related products, see these documents:
- Getting Started with Cisco Network Assistant
- Release Notes for Cisco Network Assistant
- Network Admission Control Software Configuration Guide

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

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.

© 2011–2019 Cisco Systems, Inc. All rights reserved.