# Release Notes for Cisco IOS Release 12.2SX

**September 13, 2013**

This publication applies to these releases:

- Release 12.2(33)SXJ and rebuilds
- Release 12.2(33)SXI and rebuilds
- Release 12.2(33)SXH and rebuilds

This publication applies to these platforms:

- CAT6000-VS-S720-10G/MSFC3
- CAT6000-SUP720/MSFC3
- CAT6000-SUP32/MSFC2A
- ME6524 (not supported in Release 12.2(33)SXJ and later releases)

See this product bulletin for information about the standard maintenance and extended maintenance 12.2SX releases:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd804f0694.html

These release notes are for Cisco IOS Release 12.2(33)SXH and later releases. If you are running a release earlier than Release 12.2(33)SXH, refer to this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html

The most current version of this document is available at this URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html

**Tip** For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the Technical Documentation Ideas forum

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

**Caution** Cisco IOS running on the switch processor and the route processor supports redundant configurations where the switch processor and the route processor are identical. If they are not identical, one switch processor and the route processor will boot first and become active and hold the other in a reset condition.

# Chronological List of Releases

**Note** See the "Hierarchical List of Releases" section on page 3 for information about parent releases.

This is a chronological list of the 12.2SX releases ending with Release 12.2(33)SXH:

- 13 Sep2013—Release 12.2(33)SXI12
- 23 Jul 2013—Release 12.2(33)SXJ6
- 25 Feb 2013—Release 12.2(33)SXI11
- 08 Feb 2013—Release 12.2(33)SXJ5
- 18 Sep 2012—Release 12.2(33)SXI10
- 31 Aug 2012—Release 12.2(33)SXJ4
- 25 Apr 2012—Release 12.2(33)SXJ3
- 02 Mar 2012—Release 12.2(33)SXI9
- 19 Dec 2011—Release 12.2(33)SXJ2
- 07 Dec 2011—Release 12.2(33)SXI8a
- 03 Nov 2011—Release 12.2(33)SXI8
- 23 Sep 2011—Release 12.2(33)SXH8b
- 26 Jul 2011—Release 12.2(33)SXI7
- 30 Jun 2011—Release 12.2(33)SXJ1
- 31 Mar 2011—Release 12.2(33)SXI6
- 23 Mar 2011—Release 12.2(33)SXH8a
- 21 Mar 2011—Release 12.2(33)SXJ
- 29 Oct 2010—Release 12.2(33)SXI5
- 05 Oct 2010—Release 12.2(33)SXH8
- 22 Jul 2010—Release 12.2(33)SXI4a
- 09 Jun 2010—Release 12.2(33)SXI4
- 15 Mar 2010—Release 12.2(33)SXH7
- 04 Nov 2009—Release 12.2(33)SXI3
- 21 Oct 2009—Release 12.2(33)SXH6
- 03 Sep 2009—Release 12.2(33)SXI2a
- 17 Jul 2009—Release 12.2(33)SXI2
- 20 Apr 2009—Release 12.2(33)SXH5
- 31 Mar 2009—Release 12.2(33)SXI1

- 14 Nov 2008—Release 12.2(33)SXH4
- 11 Nov 2008—Release 12.2(33)SXI
- 29 Sep 2008—Release 12.2(33)SXH3a
- 29 Jul 2008—Release 12.2(33)SXH3
- 28 Apr 2008—Release 12.2(33)SXH2a
- 31 Mar 2008—Release 12.2(33)SXH2
- 18 Jan 2008—Release 12.2(33)SXH1
- 20 Aug 2007—Release 12.2(33)SXH

# Hierarchical List of Releases

This list shows the relationship between releases:

- Release 12.2(33)SXJ6:
  - Date of release: 23 Jul 2013
  - Based on Release 12.2(33)SXJ5
- Release 12.2(33)SXJ5:
  - Date of release: 08 Feb 2013
  - Based on Release 12.2(33)SXJ4
- Release 12.2(33)SXJ4:
  - Date of release: 31 Aug 2012
  - Based on Release 12.2(33)SXJ3
- Release 12.2(33)SXJ3:
  - Date of release: 25 Apr 2012
  - Based on Release 12.2(33)SXJ2
- Release 12.2(33)SXJ2:
  - Date of release: 19 Dec 2011
  - Based on Release 12.2(33)SXJ1 and 12.2(33)SXI8a
- Release 12.2(33)SXJ1:
  - Date of release: 30 Jun 2011
  - Based on Release 12.2(33)SXJ and 12.2(33)SXI6
- Release 12.2(33)SXJ:
  - Date of release: 21 Mar 2011
  - Based on Release 12.2(33)SXI5
- Release 12.2(33)SXI12:
  - Date of release: 13 Sep 2013
  - Based on Release 12.2(33)SXI11

- Release 12.2(33)SXI11:
  - Date of release: 25 Feb 2013
  - Based on Release 12.2(33)SXI10
- Release 12.2(33)SXI10:
  - Date of release: 18 Sep 2012
  - Based on Release 12.2(33)SXI9
- Release 12.2(33)SXI9:
  - Date of release: 02 Mar 2012
  - Based on Release 12.2(33)SXI8a
- Release 12.2(33)SXI8a:
  - Date of release: 07 Dec 2011
  - Based on Release 12.2(33)SXI8
- Release 12.2(33)SXI8:
  - Date of release: 03 Nov 2011
  - Based on Release 12.2(33)SXI7
- Release 12.2(33)SXI7:
  - Date of release: 26 Jul 2011
  - Based on Release 12.2(33)SXI6
- Release 12.2(33)SXI6:
  - Date of release: 31 Mar 2011
  - Based on Release 12.2(33)SXI5
- Release 12.2(33)SXI5:
  - Date of release: 29 Oct 2010
  - Based on Release 12.2(33)SXI4a
- Release 12.2(33)SXI4a:
  - Date of release: 22 Jul 2010
  - Based on Release 12.2(33)SXI4
- Release 12.2(33)SXI4:
  - Date of release: 09 Jun 2010
  - Based on Release 12.2(33)SXI3
- Release 12.2(33)SXI3:
  - Date of release: 04 Nov 2009
  - Based on Release 12.2(33)SXI2a
- Release 12.2(33)SXI2a:
  - Date of release: 03 Sep 2009
  - Based on Release 12.2(33)SXI2

- Release 12.2(33)SXI2:
  - Date of release: 17 Jul 2009
  - Based on Release 12.2(33)SXI1
- Release 12.2(33)SXI1:
  - Date of release: 31 Mar 2009
  - Based on Release 12.2(33)SXI
- Release 12.2(33)SXI:
  - Date of release: 11 Nov 2008
  - Based on Release 12.2(33)SXH3a
- Release 12.2(33)SXH8b:
  - Date of release: 23 Sep 2011
  - Based on Release 12.2(33)SXH8a
- Release 12.2(33)SXH8a:
  - Date of release: 23 Mar 2011
  - Based on Release 12.2(33)SXH8
- Release 12.2(33)SXH8:
  - Date of release: 05 Oct 2010
  - Based on Release 12.2(33)SXH7
- Release 12.2(33)SXH7:
  - Date of release: 15 Mar 2010
  - Based on Release 12.2(33)SXH6
- Release 12.2(33)SXH6:
  - Date of release: 21 Oct 2009
  - Based on Release 12.2(33)SXH5
- Release 12.2(33)SXH5:
  - Date of release: 20 Apr 2009
  - Based on Release 12.2(33)SXH4
- Release 12.2(33)SXH4:
  - Date of release: 14 Nov 2008
  - Based on Release 12.2(33)SXH3a
- Release 12.2(33)SXH3a:
  - Date of release: 29 Sep 2008
  - Based on Release 12.2(33)SXH3
- Release 12.2(33)SXH3:
  - Date of release: 29 Jul 2008
  - Based on Release 12.2(33)SXH2a

- Release 12.2(33)SXH2a:
  - Date of release: 28 Apr 2008
  - Based on Release 12.2(33)SXH2
- Release 12.2(33)SXH2:
  - Date of release: 31 Mar 2008
  - Based on Release 12.2(33)SXH1 and Release 12.2(18)SXF13
- Release 12.2(33)SXH1:
  - Date of release: 18 Jan 2008
  - Based on Release 12.2(33)SXH and Release 12.2(18)SXF12
- Release 12.2(33)SXH:
  - Date of release: 20 Aug 2007
  - Based on Release 12.2(18)SXF10

This publication does not describe features that are available in Release 12.2, Release 12.2 T, Release 12.2 S, or other Release 12.2 early deployment releases.

For a list of the Release 12.2 caveats that apply to Release 12.2SX, see this publication:

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

For a list of the Release 12.2 S caveats that apply to Release 12.2SX, see this publication:

http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html

# Universal Boot Loader Image

A new supervisor engine contains one of the following initial software images:

- Cisco IOS software
- Catalyst operating system software
- Universal Boot Loader (UBL) software

The UBL software is a minimal network-aware image that can download and install either a Cisco IOS image or a Catalyst operating system image from a running active supervisor engine in the same chassis.

When newly installed as a standby supervisor engine in a redundant application, a supervisor engine running the UBL software automatically attempts to copy the image of the running active supervisor engine in the same chassis. This feature requires the active supervisor engine to be running either Cisco IOS software Release 12.2SXH or later, or Catalyst operating system software Release 8.6(1) or later.

**Note** When a standby supervisor engine copies a Catalyst operating system software image using UBL, the downloaded image will not include the Multilayer Switch Feature Card (MSFC) software. A Cisco IOS software image that is downloaded using UBL will include the MSFC software.

# FPD Image Packages

**Note**

- Field Programmable Device (FPD) image packages were first introduced on the Catalyst 6500 series switches and Cisco 7600 series routers in Release 12.2(18)SXE.
- FPD image packages update FPD images. If a discrepancy exists between an FPD image and the Cisco IOS image, the module that has the FPD discrepancy is deactivated until the discrepancy is resolved.

These sections describe FPD packages:


- FPD-Image Dependant Modules, page 7
- FPD Upgrades, page 7


## FPD-Image Dependant Modules

These modules use FPD images:

- Shared Port Adapter (SPA) Interface Processors (SIPs)
- Shared Port Adapters

## FPD Upgrades

See this publication:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

# Cisco IOS Software Modularity

**Note**

- Release 12.2(33)SXJ and later releases do not support Cisco IOS Software Modularity.
- With redundant supervisor engines, eFSU upgrade from a Cisco IOS Software Modularity image to a Release 12.2(33)SXJ image might result in a significant delay before the switch becomes active; the switch will be in the RPR redundancy mode.

These sections describe Cisco IOS Software Modularity:


- Cisco IOS Software Modularity Documentation, page 8
- Cisco IOS Software Modularity Unsupported Features, page 8

## Cisco IOS Software Modularity Documentation

See these publications for information about Cisco IOS Software Modularity:

- Cisco IOS Software Modularity Installation and Configuration:

  http://www.cisco.com/en/US/docs/ios/swmod/configuration/guide/sw_mod_instl_cfg.html
- Cisco IOS Software Modularity Command Reference:

  http://www.cisco.com/en/US/docs/ios/swmod/command/reference/sm_book.html
- Embedded Event Manager:

  http://www.cisco.com/en/US/docs/ios/12_4t/netmgmt/configuration/guide/t_eemo.html

## Cisco IOS Software Modularity Unsupported Features

Release 12.2(33)SXI4 and later releases do not support Cisco IOS Software Load Balancing (SLB) with Cisco IOS Modularity images.

See the *Cisco IOS Software Modularity Command Reference* "Introduction" for detailed information about specific commands that are not supported in Cisco IOS Software Modularity images.

# Troubleshooting

These sections describes troubleshooting guidelines for the Catalyst 6500 series switch configuration:


- System Troubleshooting, page 8
- Module Troubleshooting, page 9
- VLAN Troubleshooting, page 9
- Spanning Tree Troubleshooting, page 9
- Additional Troubleshooting Information, page 11


**Note** To attempt recovery from MSFC ROMMON, enter the **confreg 0x2102** and **reset** ROMMON commands.

## System Troubleshooting

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- After you initiate a switchover from the active supervisor engine to the redundant supervisor engine, or when you insert a redundant supervisor engine in an operating switch, always wait until the supervisor engines have synchronized and all modules are online before you remove or insert modules or supervisor engines or perform another switchover.
- If you have an interface whose speed is set to **auto** connected to another interface whose speed is set to a fixed value, configure the interface whose speed is set to a fixed value for half duplex. Alternately, you can configure both interfaces to a fixed-value speed and full duplex.

# Module Troubleshooting

This section contains troubleshooting guidelines for module problems:

- When you hot insert a module into a chassis, be sure to use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 6500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, make sure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the autonegotiating port will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

# VLAN Troubleshooting

**Note** Catalyst 6500 series switches do not support ISL-encapsulated Token Ring frames. To support trunked Token Ring traffic in your network, make trunk connections directly between switches that support ISL-encapsulated Token Ring frames. When a Catalyst 6500 series switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

Although DTP is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems that might be caused by a switch acting on these forwarded DTP frames, do the following:

- For interfaces connected to devices that do not support DTP, in which trunking is not currently being used, configure interfaces with the **switchport mode access** command, which puts the interface into access mode and sends no DTP frames.
- When manually enabling trunking on a link to devices that do not support DTP, use the **switchport nonegotiate** and **switchport mode trunk** commands, which puts the interface into trunking mode without sending DTP frames.

# Spanning Tree Troubleshooting

The Spanning Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, switches receive spanning tree bridge protocol data units (BPDUs) periodically from neighboring switches. You can configure the frequency with which BPDUs are received by entering the **spanning-tree vlan** *vlan_ID* **hello-time** command (the default frequency is set to 2 seconds). If a switch does not receive a BPDU in the time period defined by the **spanning-tree vlan** *vlan_ID* **max-age** command (20 seconds by default), the blocked port transitions to the listening state, the learning state, and to the forwarding state. As it transitions, the switch waits for the time period specified by the **spanning-tree vlan** *vlan_ID* **forward-time** command (15 seconds by default) in each of these intermediate states. If a blocked spanning tree interface does not receive BPDUs from its neighbor within 50 seconds, it moves into the forwarding state.

**Note** We do not recommend using the UplinkFast feature on switches with more than 20 active VLANs. The convergence time might be unacceptably long with more than 20 active VLANs.

To debug STP problems, follow these guidelines:

- The **show vlan virtual-port** command displays the number of virtual interfaces.
- These maximum numbers of virtual interfaces are supported:

| Per-switch limits: | MST | RPVST+ | PVST+ |
|---|---|---|---|
| • These per-switch limits apply to the following:<br>– Release 12.2(33)SXI and later releases<br>– Supervisor Engine 720-10GE<br>– Supervisor Engine 720 | 100,000 total<br>**Note** Messages with the per-switch limits from earlier releases are still displayed in Release 12.2(33)SXI. Messages for the per-switch limits in effect in Release 12.2(33)SXI are displayed in Release 12.2(33)SXI1 and later releases. (CSCsx62912) | 12,000 total | 15,000 total |
| • All other releases and supervisor engines: | 50,000 total | 10,000 total | 13,000 total |

| Per-module limits: | 6,000 | 1,800 | 1,800 |
|---|---|---|---|

**Note**

- In Release 12.2(33)SXI1 and later releases, these limits do not apply to WS-X67xx and WS-X65xx switching modules. (CSCsu30263)
- 10/100 Mb and 100 Mbps switching modules support a maximum of 1,200 logical interfaces per module

**Note** Cisco IOS software displays a message if you exceed the maximum number of virtual interfaces.

- After a switchover from the active to the redundant supervisor engine, the ports on the redundant supervisor engine take longer to come up than other ports.
- Record all spanning tree-blocked ports in each switch in your network. For each of the spanning tree-blocked ports, record the output of the **show interface** command. Check to see if the port has registered many alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs. If the input queue counter is incrementing continuously, the port is losing input packets because of a lack of receive buffers. This problem can also cause the port to drop incoming BPDUs.
- On a blocked spanning tree port, check the duplex configuration to ensure that the port duplex is set to the same type as the port of its neighboring device.
- On trunks, make sure that the trunk configuration is set properly on both sides of the link.
- On trunks, if the neighboring device supports it, set duplex to full on both sides of the link to prevent any collisions under heavy traffic conditions.

## Additional Troubleshooting Information

For additional troubleshooting information, refer to the publications at this URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_troubleshoot_and_alerts.html

# System Software Upgrade Instructions

See this publication:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a0080116ff0.shtml

## Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

# Notices

The following notices pertain to this software license.

## OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

## License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

**OpenSSL License:**

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

**Original SSLeay License:**

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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

This document is to be used in conjunction with the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* and the *Catalyst 6500 Series Cisco IOS Command Reference* publications.

---

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. (1110R)

© 2006–2013, Cisco Systems, Inc.
All rights reserved.

---

# Supported Hardware

These sections describe the hardware supported in Release 12.2(33)SXH and later releases:


- Supervisor Engines, page 16
- Policy Feature Cards, page 24
- Distributed and Centralized Forwarding Cards, page 30
- 10-Gigabit Ethernet Switching Modules, page 38
- Gigabit Ethernet Switching Modules, page 51
- 10/100/1000 Ethernet Switching Modules, page 59
- Fast Ethernet Switching Modules, page 66
- Ethernet/Fast Ethernet (10/100) Switching Modules, page 68
- Power over Ethernet Daughtercards, page 73
- Transceivers, page 75
- Shared Port Adapter (SPA) Interface Processors (SIPs), page 84
- Shared Port Adapters (SPAs), page 85
- Services SPA Carrier (SSC) and Services SPAs, page 89
- Enhanced FlexWAN Module, page 90
- Enhanced FlexWAN Module Port Adapters, page 90
- Service Modules, page 91
- Fan Trays, page 100
- Power Supplies, page 100
- Chassis, page 103
- Cisco ME 6500 Series Ethernet Switches (ME6524), page 110

**Note**

- Enter the **show power** command to display current system power usage.
- Flash Memory Device Summary
  - **bootflash:** on the RP of all supervisor engines.
  - **sup-bootdisk:** on the SP of these supervisor engines:

    Supervisor Engine 720-10GE.

    Supervisor Engine 720 with a CompactFlash adapter and CompactFlash card sold by Cisco Systems, Inc., for use in Supervisor Engine 720-10GE.

    Supervisor Engine 32.
  - **sup-bootflash:** on the SP of these supervisor engines:

    Supervisor Engine 720 without a CompactFlash adapter and CompactFlash card sold by Cisco Systems, Inc., for use in Supervisor Engine 720.

    ME 6500.
  - **disk0:** on these supervisor engines:

    Supervisor Engine 720-10GE.

    Supervisor Engine 720.

    Supervisor Engine 32.

    ME 6500.
  - **disk1:** on a Supervisor Engine 720.

# Supervisor Engines


- Supervisor Engine 720-10GE (CAT6000-VS-S720-10G/MSFC3), page 16
- Supervisor Engine 720 (CAT6000-SUP720/MSFC3), page 18
- Supervisor Engine 32 (CAT6000-SUP32/MSFC2A), page 22
- Cisco ME 6500 Series Ethernet Switches (ME6524), page 24


**Note** For information about DRAM requirements on all supervisor engines, see this publication:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/qa_c67_457347.html

## Supervisor Engine 720-10GE (CAT6000-VS-S720-10G/MSFC3)


- Supervisor Engine 720-10GE Common Features, page 17
- Supervisor Engine 720-10GE with PFC3C and PFC3CXL, page 18
- Supervisor Engine 720-10GE Restrictions, page 18

### Supervisor Engine 720-10GE Common Features

- Switch processor (SP):
  - Internal 1-GB CompactFlash card (**sup-bootdisk:**).
  - 1-GB DRAM.
- Route processor (RP):
  - Internal 64-MB bootflash.
  - 1-GB DRAM.
- One of these:
  - Policy Feature Card 3CXL (PFC3CXL).
  - Policy Feature Card 3C (PFC3C).
  - See the "Policy Feature Cards" section on page 24.
- Integrated 720-Gbps Switch Fabric.
- One external slot:
  - **disk0:**
  - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 720-10GE.
- Console port—EIA/TIA-232 (RS-232) port.
- Ports 1 and 2:
  - QoS architecture: **2q4t/1p3q4t**
  - Support for Gigabit Ethernet SFP Modules
- Port 3:
  - 10/100/1000 Mbps RJ-45
  - QoS architecture: **2q4t/1p3q4t**
- Ports 4 and 5:
  - Support for 10-Gigabit Ethernet X2 tranceivers
  - QoS architecture: **2q4t/1p3q4t** or **8q4t/1p7q4t**

**Note** The 1-Gigabit Ethernet ports and the 10-Gigabit Ethernet ports have the same QoS port architecture (**2q4t/1p3q4t**) unless you disable the 1-Gigabit Ethernet ports with the **mls qos 10g-only** global configuration command, which is required to configure DSCP-based queueing. With the 1-Gigabit Ethernet ports disabled, the QoS port architecture of the 10-Gigabit Ethernet ports is **8q4t/1p7q4t**.

- One port group: ports 1 through 5.
- Two Universal Serial Bus (USB) 2.0 ports (not currently enabled)

### Supervisor Engine 720-10GE with PFC3C and PFC3CXL

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **VS-S720-10G-3CXL** | Supervisor Engine 720-10GE with PFC3CXL | 12.2(33)SXH[1] |
| **VS-S720-10G-3C** | Supervisor Engine 720-10GE with PFC3C | 12.2(33)SXH[1] |

1. If there are no DFC-equipped modules installed, certain configurations require Release 12.2(33)SXH1 or later and impose configuration restrictions that are described in CSCsj95733.

### Supervisor Engine 720-10GE Restrictions

- In RPR redundancy mode, the ports on a Supervisor Engine 720-10GE in standby mode are disabled.
- Supervisor Engine 720-10GE requires a high-capacity fan tray (see the "Fan Trays" section on page 100). All E-series chassis have a high-capacity fan tray.
- There are no memory-only upgrade options for the Supervisor Engine 720-10GE.

## Supervisor Engine 720 (CAT6000-SUP720/MSFC3)


- Supervisor Engine 720 Common Features, page 18
- Supervisor Engine 720 with PFC3BXL, page 19
- Supervisor Engine 720 with PFC3B, page 20
- Supervisor Engine 720 with PFC3A, page 21


### Supervisor Engine 720 Common Features

- Integrated 720-Gbps Switch Fabric
- Internal 64-MB bootflash device (**sup-bootflash:**) or CompactFlash card (sup-bootdisk:), 512 MB or larger.
  - As an upgrade, WS-CF-UPG=
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_17277.html
- Two external slots (disk0: and disk1:) for CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 720.

**Note** Some Supervisor Engine 720 Release 12.2SX images are larger than the bootflash device and must be stored on a CompactFlash card (sup-bootdisk: or disk0: or disk1:).

- Two Ethernet uplink ports:
  - 512-KB packet buffer per port
  - Port 1—Gigabit Interface Converter (GBIC)
  - Port 2—Configurable as either:
    - Gigabit Interface Converter (GBIC)
    - 10/100/1000 Mbps RJ-45
- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Port grouping:
  - Number of ports: 2
  - Number of port groups: 1
  - Port ranges per port group: 1–2
- Supervisor Engine 720 requires a high-capacity fan tray (see the "Fan Trays" section on page 100). All E-series chassis have a high-capacity fan tray.

### Supervisor Engine 720 with PFC3BXL

**Note** If you install WS-SUP720-3BXL=, upgrade the memory on any DFC3-equipped switching modules. See this document for DFC3 memory upgrades:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-SUP720-3BXL** | Supervisor Engine 720 with PFC3BXL:<br>• Switch processor (SP):<br>– Internal 64-MB bootflash device (**sup-bootflash:**) or internal CompactFlash card (sup-bootdisk:)<br>– 1-GB or larger DRAM<br>• Route processor (RP):<br>– 1-GB or larger DRAM<br>– 64-MB bootflash<br>• Policy Feature Card 3BXL (PFC3BXL)—See the "Policy Feature Cards" section on page 24. | 12.2(17b)SXA |

### Supervisor Engine 720 with PFC3B

**Note**

- See this document for DFC3 memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html

- Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3.
  - If you install WS-F6K-PFC3BXL=, upgrade the memory on any DFC3-equipped switching modules.
  - See this publication for more information about WS-F6K-PFC3BXL=:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-SUP720-3B** | Supervisor Engine 720 with PFC3B:<br>• Switch processor (SP):<br>– Internal 64-MB bootflash device (**sup-bootflash:**) or internal CompactFlash card (sup-bootdisk:)<br>– 512-MB or larger DRAM<br>• Route processor (RP):<br>– 64-MB bootflash<br>– 512-MB or larger DRAM<br>• Policy Feature Card 3B (PFC3B)—See the "Policy Feature Cards" section on page 24 | 12.2(17d)SXB1 |

### Supervisor Engine 720 with PFC3A

**Note**

- See this document for DFC3 memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Use WS-F6K-PFC3B= to upgrade a WS-SUP720 with a PFC3B. Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720 with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3.
  - If you install WS-F6K-PFC3BXL=, upgrade the memory on any DFC3-equipped switching modules.
  - See this publication for more information about WS-F6K-PFC3BXL=:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html
- Except with WS-F6K-PFC3B= or WS-F6K-PFC3BXL=, do not upgrade the memory on the switch processor or the route processor on a WS-SUP720.

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-SUP720** | Supervisor Engine 720 with PFC3A:<br>• Switch processor<br>– Internal 64-MB bootflash device (**sup-bootflash:**) or internal 512 MB CompactFlash card (sup-bootdisk:)<br>– 512-MB DRAM<br>• Route processor:<br>– 64-MB bootflash<br>– 512-MB DRAM<br>• Policy Feature Card 3A (PFC3A; see the "Policy Feature Cards" section on page 24) | 12.2(14)SX |

# Supervisor Engine 32 (CAT6000-SUP32/MSFC2A)


- Supervisor Engine 32 Restrictions, page 22
- Supervisor Engine 32 Features, page 23


## Supervisor Engine 32 Restrictions

- Supervisor Engine 32 requires a high-capacity fan tray (see the "Fan Trays" section on page 100). All E-series chassis have a high-capacity fan tray.
- In some chassis, Supervisor Engine 32 requires a high-capacity power supply (see the "Power Supplies" section on page 100).
- Supervisor Engine 32 cannot support this hardware:
  - DFCs (switching modules with DFCs do not power up with a Supervisor Engine 32)
  - WS-X6700 series switching modules
  - WS-X6816-GBIC switching modules
  - The WS-SVC-WISM-1-K9 Wireless Services Module (WiSM)
  - 7600-SIP-600 SPA Interface Processor-600 and SPAs supported only in 7600-SIP-600.
- Supervisor Engine 32 does not support this hardware:
  - WS-F6K-PFC3A Policy Feature Card 3A (PFC3A)
  - WS-F6K-PFC3BXL Policy Feature Card 3BXL (PFC3BXL)
  - CISCO7603 3-slot chassis
- Supervisor Engine 32 cannot support these software features and commands:
  - Egress multicast replication
  - Multicast replication mode detection
  - All fabric configuration commands

## Supervisor Engine 32 Features

**Note**

- See this publication for Supervisor Engine 32 hardware information:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Module_Installation/Sup_Eng_Guide/supe_gd.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-SUP32-10GE-3B**<br>**WS-SUP32-GE-3B** | Supervisor Engine 32:<br>• One 10/100/1000 Mbps RJ-45 port<br>• WS-SUP32-10GE<br>– Two 10-Gigabit Ethernet ports<br>– Requires XENPAKs<br>• WS-SUP32-GE<br>– Eight SFP ports<br>– Requires Gigabit or 10/100/1000 Mbps Ethernet SFPs<br>• QoS port architecture (Rx/Tx): **2q8t/1p3q8t**<br>• One external slot (**disk0:**) for CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 32<br>• Switch processor<br>– Internal 256 MB CompactFlash card (**sup-bootdisk:**)<br>– 512-MB or more DRAM (some images require more DRAM)<br>• Route processor:<br>– Internal 64-MB bootflash<br>– 512-MB or more DRAM (some images require more DRAM)<br>• Policy Feature Card 3B (PFC3B)—See the "Policy Feature Cards" section on page 24)<br>• Two Universal Serial Bus (USB) 2.0 ports (not currently enabled) | 12.2(18)SXF |

## Cisco ME 6500 Series Ethernet Switches (ME6524)

| Product ID (append "=" for spares) | Product Description | Minimum Software Version |
|---|---|---|
| **ME-C6524GS-8S**<br>**ME-C6524GT-8S** | Cisco ME 6500 Series Ethernet switches:<br>• Switch processor (SP):<br>– 256-MB DRAM<br>– 128-MB bootflash<br>• Policy Feature Card 3C (PFC3C):<br>– Supports a theoretical maximum of 96 K MAC addresses (64 K MAC addresses recommended maximum).<br>– The PFC3C operates in PFC3C mode. Enter the **show platform hardware pfc mode** command to display the PFC3 mode.<br>• Route processor (RP)—Multilayer Switch Feature Card 2A (MSFC2A):<br>– 512-MB DRAM<br>– 64-MB bootflash<br>• Fan tray: FAN-C6524<br>• Power supplies: PWR-400W-DC<br>• 64 chassis MAC addresses<br>• Eight Gigabit Ethernet SFP ports:<br>– Requires Gigabit Ethernet SFPs<br>– 1 port group: ports 25–32<br>– QoS port architecture (Rx/Tx): **2q8t/1p3q8t**<br>• ME-C6524GS-8S:<br>– 24 Gigabit Ethernet SFP ports (requires Gigabit Ethernet SFPs)<br>– 4 port groups: ports 1–6, 7–12, 13–18, 19–24<br>– QoS port architecture (Rx/Tx): **1q2t/1p3q8t**<br>• ME-C6524GT-8S:<br>– 24 10/100/1000 Mbps RJ-45 Ethernet ports<br>– 4 port groups: ports 1–6, 7–12, 13–18, 19–24<br>– QoS port architecture (Rx/Tx): **1q2t/1p3q8t** | 12.2(33)SXH<br>Not supported in 12.2(33)SXJ and later releases. |

**Note** See this publication for Cisco ME 6500 Series Ethernet switch hardware information:

http://www.cisco.com/en/US/products/ps6845/prod_installation_guides_list.html

# Policy Feature Cards


- Policy Feature Card Guidelines and Restrictions, page 25
- Policy Feature Card 3CXL, page 27

- Policy Feature Card 3C, page 28
- Policy Feature Card 3BXL, page 28
- Policy Feature Card 3B, page 28
- Policy Feature Card 3A, page 29


## Policy Feature Card Guidelines and Restrictions

- The PFC3C supports a theoretical maximum of 96 K MAC addresses (64 K MAC addresses recommended maximum).
- The PFC3A, PFC3B, and PFC3BXL support a theoretical maximum of 64 K MAC addresses (32 K MAC addresses recommended maximum).
- The PFC3 partitions the hardware FIB table to route IPv4 unicast, IPv4 multicast, MPLS, and IPv6 unicast and multicast traffic in hardware. Traffic for routes that do not have entries in the hardware FIB table are processed by the route processor in software.

  The defaults for XL mode are:

  – IPv4 unicast and MPLS—512,000 routes

  – IPv4 multicast and IPv6 unicast and multicast—256,000 routes

  The defaults for Non-XL mode are:

  – IPv4 unicast and MPLS—192,000 routes

  – IPv4 multicast and IPv6 unicast and multicast—32,000 routes

  **Note** The size of the global internet routing table plus any local routes might exceed the non-XL mode default partition sizes.

  These are the theoretical maximum numbers of routes for the supported protocols (the maximums are not supported simultaneously):

  – XL mode:

    • IPv4 and MPLS—Up to 1,007,000 routes

    • IPv4 multicast and IPv6 unicast and multicast—Up to 503,000 routes

  – Non-XL mode:

    • IPv4 and MPLS—Up to 239,000 routes

    • IPv4 multicast and IPv6 unicast and multicast—Up to 119,000 routes

  Enter the mls cef maximum-routes command to repartition the hardware FIB table. IPv4 unicast and MPLS require one hardware FIB table entry per route. IPv4 multicast and IPv6 unicast and multicast require two hardware FIB table entries per route. Changing the partition for one protocol makes corresponding changes in the partitions of the other protocols. You must enter the **reload** command to put configuration changes made with the **mls cef maximum-routes** command into effect.

  **Note** With a non-XL-mode system, if your requirements cannot be met by repartitioning the hardware FIB table, upgrade components as necessary to operate in XL mode.

- You cannot use one type of PFC3 on one supervisor engine and a different type on the other supervisor engine for redundancy. You must use identical policy feature cards for redundancy.

- PFC3A—These restrictions apply to a configuration with a PFC3A and these DFCs:
  - PFC3A and DFC3A—No restrictions (PFC3A mode; does not support virtual switch mode).
  - PFC3A and DFC3B—The PFC3A restricts DFC3B functionality: the DFC3B functions as a DFC3A (PFC3A mode; does not support virtual switch mode).
  - PFC3A and DFC3BXL—The PFC3A restricts DFC3BXL functionality: the DFC3BXL functions as a DFC3A (PFC3A mode; does not support virtual switch mode).
  - PFC3A and DFC3C—The PFC3A restricts DFC3C functionality: the DFC3C functions as a DFC3A (PFC3A mode; does not support virtual switch mode).
  - PFC3A and DFC3CXL—The PFC3A restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3A (PFC3A mode; does not support virtual switch mode).
- PFC3B—These restrictions apply to a configuration with a PFC3B and these DFCs:
  - PFC3B and DFC3A—PFC3B functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3B functions as a PFC3A (PFC3A mode; does not support virtual switch mode).
  - PFC3B and DFC3B—No restrictions (PFC3B mode; does not support virtual switch mode).
  - PFC3B and DFC3BXL—The PFC3B restricts DFC3BXL functionality: after a reload with a DFC3BXL-equipped module installed, the DFC3BXL functions as a DFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3B and DFC3C—The PFC3B restricts DFC3C functionality: the DFC3C functions as a DFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3B and DFC3CXL—The PFC3B restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3B (PFC3B mode; does not support virtual switch mode).
- PFC3BXL—These restrictions apply to a configuration with a PFC3BXL and these DFCs:
  - PFC3BXL and DFC3A—PFC3BXL functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3BXL functions as a PFC3A (PFC3A mode; does not support virtual switch mode).
  - PFC3BXL and DFC3B—PFC3BXL functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3BXL functions as a PFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3BXL and DFC3BXL—No restrictions (PFC3BXL mode; does not support virtual switch mode).
  - PFC3BXL and DFC3C—Each restricts the functionality of the other: the PFC3BXL functions as a PFC3B and the DFC3C functions as a DFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3BXL and DFC3CXL—The PFC3BXL restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3BXL (PFC3BXL mode; does not support virtual switch mode).
- PFC3C—These restrictions apply to a configuration with a PFC3C and these DFCs:
  - PFC3C and DFC3A—PFC3C functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3C functions as a PFC3A (PFC3A mode; does not support virtual switch mode).
  - PFC3C and DFC3B—PFC3C functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3C functions as a PFC3B (PFC3B mode; does not support virtual switch mode).

  - PFC3C and DFC3BXL—PFC3C functionality is restricted by the DFC3BXL: after a reload with a DFC3BXL-equipped module installed, the PFC3C functions as a PFC3BXL (PFC3BXL mode; does not support virtual switch mode).
  - PFC3C and DFC3C—No restrictions (PFC3C mode).
  - PFC3C and DFC3CXL—The PFC3C restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3C (PFC3C mode).
- PFC3CXL—These restrictions apply to a configuration with a PFC3CXL and these DFCs:
  - PFC3CXL and DFC3A—PFC3CXL functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3CXL functions as a PFC3A (PFC3A mode; does not support virtual switch mode).
  - PFC3CXL and DFC3B—PFC3CXL functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3CXL functions as a PFC3B (PFC3B mode; does not support virtual switch mode).
  - PFC3CXL and DFC3BXL—PFC3CXL functionality is restricted by the DFC3BXL: after a reload with a DFC3BXL-equipped module installed, the PFC3CXL functions as a PFC3BXL (PFC3BXL mode; does not support virtual switch mode).
  - PFC3CXL and DFC3C—PFC3CXL functionality is restricted by the DFC3C: after a reload with a DFC3C-equipped module installed, the PFC3CXL functions as a PFC3C (PFC3C mode).
  - PFC3CXL and DFC3CXL—No restrictions (PFC3CXL mode).
- Switching modules that you install after bootup that are equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode remain powered down.
- You must reboot to use a switching module equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode.
- Enter the **show platform hardware pfc mode** command to display the PFC mode.

## Policy Feature Card 3CXL

**Note** Use VS-F6K-PFC3CXL= to upgrade a VS-S720-10G-3C with a PFC3CXL. See this publication for more information:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| VS-F6K-PFC3CXL | Policy Feature Card 3CXL (PFC3CXL) | |
| | Supported only with Supervisor Engine 720-10GE | 12.2(33)SXH |

## Policy Feature Card 3C

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| VS-F6K-PFC3C<br>ME-C6524-PFC3C | Policy Feature Card 3C (PFC3C) | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Cisco ME 6500 Series Ethernet switches | 12.2(33)SXH |

## Policy Feature Card 3BXL

**Note** Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720 or WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3. See this publication for more information:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| WS-F6K-PFC3BXL | Policy Feature Card 3BXL (PFC3BXL) | |
| | Supported only with Supervisor Engine 720 | 12.2(17b)SXA |

## Policy Feature Card 3B

**Note** Use WS-F6K-PFC3B= to upgrade a WS-SUP720 with a PFC3B. See this publication for more information:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| WS-F6K-PFC3B | Policy Feature Card 3B (PFC3B) | |
| | With Supervisor Engine 720 | 12.2(17d)SXB1 |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## Policy Feature Card 3A

**Note** WS-F6K-PFC3A is available only on WS-SUP720. It is not orderable.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-F6K-PFC3A** | Policy Feature Card 3A (PFC3A) | |
| | Supported only with Supervisor Engine 720 | 12.2(14)SX |

# Distributed and Centralized Forwarding Cards


- Distributed Forwarding Card 3CXL, page 30
- Distributed Forwarding Card 3C, page 31
- Distributed Forwarding Card 3BXL, page 32
- Distributed Forwarding Card 3B, page 34
- Distributed Forwarding Card 3A, page 36
- Centralized Forwarding Card (WS-F6700-CFC), page 38


**Note** See the "Policy Feature Cards" section on page 24 for Policy Feature Cards (PFC) and Distributed Forwarding Card (DFC) restrictions.

## Distributed Forwarding Card 3CXL

**Note**

- WS-F6700-DFC3CXL uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3CXL upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Version** |
|---|---|---|
| **WS-F6700-DFC3CXL** | Distributed Forwarding Card 3CXL (DFC3CXL) for use on CEF720 modules | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 and all WS-X6700 series modules | 12.2(33)SXH |
| | With Supervisor Engine 720 and WS-X6708-10GE | 12.2(18)SXF5 |

## Distributed Forwarding Card 3C

**Note**

- WS-F6700-DFC3C uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3C upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Version** |
|---|---|---|
| **WS-F6700-DFC3C** | Distributed Forwarding Card 3C (DFC3C) for use on CEF720 modules | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 and all WS-X6700 series modules | 12.2(33)SXH |
| | With Supervisor Engine 720 and WS-X6708-10GE | 12.2(18)SXF5 |

## Distributed Forwarding Card 3BXL


- WS-F6700-DFC3BXL, page 32
- WS-F6K-DFC3BXL, page 33


### WS-F6700-DFC3BXL

**Note**

- WS-F6700-DFC3BXL uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3BXL upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-F6700-DFC3BXL** | Distributed Forwarding Card 3BXL (DFC3BXL) for use on CEF720 modules | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17d)SXB6 |

### WS-F6K-DFC3BXL

**Note**

- See this publication for information about WS-F6K-DFC3BXL memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Supervisor Engine 720 supports a WS-F6K-DFC3BXL on these WS-X6516-GBIC switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Use with Release 12.2(33)SXH or later requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6010.html
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-F6K-DFC3BXL** | Distributed Forwarding Card 3BXL (DFC3BXL) for use on dCEF256 and CEF256 modules | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXD3 |

## Distributed Forwarding Card 3B


- WS-F6700-DFC3B, page 34
- WS-F6K-DFC3B, page 35


### WS-F6700-DFC3B

**Note**

- WS-F6700-DFC3B uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3B upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-F6700-DFC3B** | Distributed Forwarding Card 3B (DFC3B) for use on CEF720 modules | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17d)SXB6 |

### WS-F6K-DFC3B

**Note**

- See this publication for information about WS-F6K-DFC3B memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html

- Use with Release 12.2(33)SXH or later requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6010.html

- Supervisor Engine 720 supports a WS-F6K-DFC3B on these WS-X6516-GBIC switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-F6K-DFC3B** | Distributed Forwarding Card 3B (DFC3B) for use on dCEF256 and CEF256 modules | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXD3 |

# Distributed Forwarding Card 3A


- WS-F6700-DFC3A, page 36
- WS-F6K-DFC3A, page 37


## WS-F6700-DFC3A

**Note**

- WS-F6700-DFC3A uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3A memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-F6700-DFC3A** | Distributed Forwarding Card 3A (DFC3A) for use on CEF720 modules | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17a)SX |

## WS-F6K-DFC3A

**Note**

- Not supported in virtual switch mode.
- See this publication for information about WS-F6K-DFC3A memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Use with Release 12.2(33)SXH or later requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6010.html
- Supervisor Engine 720 supports a WS-F6K-DFC3A on these WS-X6516-GBIC switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-F6K-DFC3A** | Distributed Forwarding Card 3A (DFC3A) for use on dCEF256 and CEF256 modules | |
| | Supported only with Supervisor Engine 720 | 12.2(14)SX |

## Centralized Forwarding Card (WS-F6700-CFC)

**Note**

- There are no memory upgrade options for WS-F6700-CFC.
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-F6700-CFC** | Centralized Forwarding Card (CFC) for use on CEF720 modules | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17a)SX |

# 10-Gigabit Ethernet Switching Modules


- 76-ES+XT-4TG3CXL, 76-ES+XT-4TG3C, page 39
- 76-ES+XT-2TG3CXL, 76-ES+XT-2TG3C, page 40
- 7600-ES+4TG3CXL, 7600-ES+4TG3C, page 40
- 7600-ES+2TG3CXL, 7600-ES+2TG3C, page 41
- WS-X6716-10T 16-port 10-Gigabit Ethernet Copper Switching Module, page 42
- WS-X6716-10G 16-port 10-Gigabit Ethernet X2 Switching Module, page 44
- WS-X6708-10GE 8-port 10-Gigabit Ethernet X2 Switching Module, page 46
- WS-X6704-10GE 4-port 10-Gigabit Ethernet XENPAK Switching Module, page 48
- WS-X6502-10GE 1-port 10-Gigabit Ethernet Switching Module, page 50

## 76-ES+XT-4TG3CXL, 76-ES+XT-4TG3C

**Note**

- Not supported in PFC3A mode.
- CDP is disabled by default on ES+ line card ports (CSCtk12860).

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **76-ES+XT-4TG3CXL** (has DFC3CXL)<br>**76-ES+XT-4TG3C** (has DFC3C) | Four-port Ethernet Services Plus Extended Transport (ES+XT) Line Card<br>• Four 10GE ports<br>• Dual fabric connections<br>• Network Processors (NP):<br>– Port 1: NP0<br>– Port 2: NP1<br>– Port 3: NP2<br>– Port 4: NP3<br>• Transceivers: LAN/WAN PHY, OTN/G.709 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXJ1 |
| | With Supervisor Engine 720 | |

## 76-ES+XT-2TG3CXL, 76-ES+XT-2TG3C

**Note**

- Not supported in PFC3A mode.
- CDP is disabled by default on ES+ line card ports (CSCtk12860).

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **76-ES+XT-2TG3CXL** (has DFC3CXL)<br>**76-ES+XT-2TG3C** (has DFC3C) | Two-port Ethernet Services Plus Extended Transport (ES+XT) Line Card<br>• Two 10GE ports<br>• Single fabric connection<br>• Network Processors (NP):<br>– Port 1: NP0<br>– Port 2: NP1<br>• Transceivers: LAN/WAN PHY, OTN/G.709 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXJ1 |
| | With Supervisor Engine 720 | |

## 7600-ES+4TG3CXL, 7600-ES+4TG3C

**Note**

- Not supported in PFC3A mode.
- CDP is disabled by default on ES+ line card ports (CSCtk12860).

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **7600-ES+4TG3CXL** (has DFC3CXL)<br>**7600-ES+4TG3C** (has DFC3C) | Four-port Ethernet Services Plus (ES) Line Card<br>• Four 10GE ports<br>• Dual fabric connections<br>• Network Processors (NP):<br>– Port 1: NP0<br>– Port 2: NP1<br>– Port 3: NP2<br>– Port 4: NP3 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXJ1 |
| | With Supervisor Engine 720 | |

## 7600-ES+2TG3CXL, 7600-ES+2TG3C

**Note**

- Not supported in PFC3A mode.
- CDP is disabled by default on ES+ line card ports (CSCtk12860).

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **7600-ES+2TG3CXL** (has DFC3CXL)<br>**7600-ES+2TG3C** (has DFC3C) | Two-port Ethernet Services Plus (ES) Line Card<br>• Two 10GE ports<br>• Single fabric connection<br>• Network Processors (NP):<br>– Port 1: NP0<br>– Port 2: NP1 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXJ1 |
| | With Supervisor Engine 720 | |

## WS-X6716-10T 16-port 10-Gigabit Ethernet Copper Switching Module

**Note**

- When not configured in oversubscription mode, supported in virtual switch links with Release 12.2(33)SXI and later releases.
- The orderable product IDs are WS-X6716-10T-3C and WS-X6716-10T-3CXL.
- The front panel is labeled WS-X6716-10T.
- Cisco IOS software commands display “WS-X6716-10T” with either WS-F6700-DFC3C or WS-F6700-DFC3CXL.
- To configure WS-X6716-10T port oversubscription, use the **hw-module slot** command.
- In these chassis, operation of a WS-X6716-10T switching module without over-temperature alarms is supported only with operating temperatures up to 40° C:
- WS-C6513
- CISCO7613
- WS-C6509
- OSR-7609
- WS-C6506
- CISCO7606
- Full NEBS-compliance requires support for operating temperatures up to 55° C, which is available in all other chassis that support WS-X6716-10T.
- All E-Series chassis provide NEBS compliance.
- Support in the WS-C6509-NEB-A chassis requires two FAN-MOD-09 modules.
- Not supported in the WS-C6503, CISCO7603, or WS-C6509-NEB chassis.
- In a 13-slot chassis, supported only in slots 9 through 13 and does not power up in other slots.
- Does not support ISL encapsulation.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6716-10T-3CXL** (**WS-X6716-10T** with WS-F6700-DFC3CXL)<br>**WS-X6716-10T-3C** (**WS-X6716-10T** with WS-F6700-DFC3C) | 16-port 10-Gigabit Ethernet copper (RJ-45) module<br>• dCEF720<br>• Supports egress multicast replication<br>• QoS port architecture (Rx/Tx):<br>– Oversubscription mode: **1p7q2t/1p7q4t**<br>– Performance mode: **8q4t/1p7q4t**<br>– Both modes support DSCP-based queueing<br>• Dual switch-fabric connections<br>Fabric Channel #1: ports 1–8<br>Fabric Channel #2: ports 9–16<br>• Number of ports: 16<br>Number of port groups: 4<br>Port ranges per port group: 1–4, 5–8, 9–12, 13–16 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXI4 (12.2(33)SXI4a or later recommended) |
| | With Supervisor Engine 720 | |

## WS-X6716-10G 16-port 10-Gigabit Ethernet X2 Switching Module

**Note**

- The orderable product IDs are WS-X6716-10G-3C and WS-X6716-10G-3CXL.
- The front panel is labeled WS-X6716-10GE.
- Cisco IOS software commands display "WS-X6716-10G" with either WS-F6700-DFC3C or WS-F6700-DFC3CXL.
- To configure WS-X6716-10G port oversubscription, use the **hw-module slot** command.
- In these chassis, operation of a WS-X6716-10G switching module without over-temperature alarms is supported only with operating temperatures up to 40° C:
  - WS-C6513
  - CISCO7613
  - WS-C6509
  - WS-C6509-NEB
  - OSR-7609
  - WS-C6506
  - CISCO7606

  Full NEBS-compliance requires support for operating temperatures up to 55° C, which is available in all other chassis that support WS-X6716-10G.

  **Note** All E-Series chassis provide NEBS compliance.

- Support in the WS-C6509-NEB-A chassis requires two FAN-MOD-09 modules.
- WS-X6716-10G is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6716-10G is supported only in slots 9 through 13 and does not power up in other slots.
- With Release 12.2(33)SXH1, WS-X6716-10G ports in oversubscription mode do not support VACL capture. (CSCsm46682)
- Not supported in virtual switch links with Releases earlier than Release 12.2(33)SXI.
- When not configured in oversubscription mode, supported in virtual switch links with Release 12.2(33)SXI and later releases.
- Does not support ISL encapsulation.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6716-10G-3CXL** (**WS-X6716-10G** with WS-F6700-DFC3CXL)<br>**WS-X6716-10G-3C** (**WS-X6716-10G** with WS-F6700-DFC3C) | 16-port 10-Gigabit Ethernet X2 module<br>• dCEF720<br>• Supports egress multicast replication<br>• QoS port architecture (Rx/Tx):<br>– Oversubscription mode: **1p7q2t/1p7q4t**<br>– Performance mode: **8q4t/1p7q4t**<br>– Both modes support DSCP-based queueing<br>• Dual switch-fabric connections<br>Fabric Channel #1: ports 1–8<br>Fabric Channel #2: ports 9–16<br>• Number of ports: 16<br>Number of port groups: 4<br>Port ranges per port group: 1–4, 5–8, 9–12, 13–16 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH2 |
| | With Supervisor Engine 720 | 12.2(33)SXH2 |

## WS-X6708-10GE 8-port 10-Gigabit Ethernet X2 Switching Module

**Note**

- WS-X6708-10G-3C and WS-X6708-10G-3CXL are the orderable product IDs.
- The front panel is labeled WS-X6708-10GE.
- Cisco IOS software commands display WS-X6708-10GE with either WS-F6700-DFC3C or WS-F6700-DFC3CXL.
- To configure WS-X6708-10GE port oversubscription, use the **hw-module oversubscription** command.
- In these chassis, operation of a WS-X6708-10GE switching module without over-temperature alarms is supported only with operating temperatures up to 40° C:
  - WS-C6513
  - CISCO7613
  - WS-C6509
  - WS-C6509-NEB
  - OSR-7609
  - WS-C6506
  - CISCO7606

  Full NEBS-compliance requires support for operating temperatures up to 55° C, which is available in all other chassis that support WS-X6708-10GE.

  **Note** All E-Series chassis provide NEBS compliance.

- Support in the WS-C6509-NEB-A chassis requires two FAN-MOD-09 modules.
- WS-X6708-10GE is supported in the WS-C6503-E chassis.
- WS-X6708-10GE is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6708-10GE is supported only in slots 9 through 13 and does not power up in other slots.
- WS-X6708-10GE ports do not support VACL capture. (CSCsb59015)

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-X6708-10G-3C** (**WS-X6708-10GE** with WS-F6700-DFC3C)<br>**WS-X6708-10G-3CXL** (**WS-X6708-10GE** with WS-F6700-DFC3CXL) | 8-port 10-Gigabit Ethernet X2 module<br>• dCEF720<br>• Supports egress multicast replication<br>• QoS port architecture (Rx/Tx):<br>– Oversubscription mode: **1p7q2t/1p7q4t**<br>– Performance mode: **8q4t/1p7q4t**<br>– Both modes support DSCP-based queueing<br>• Dual switch-fabric connections<br>Fabric Channel #1: Ports 2, 3, 6, 8<br>Fabric Channel #2: Ports 1, 4, 5, 7<br>• Number of ports: 8<br>Number of port groups: 8<br>Port ranges per port group: 1 port in each group | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF5 |

## WS-X6704-10GE 4-port 10-Gigabit Ethernet XENPAK Switching Module

**Note**

- WS-X6704-10GE requires one of the following:
  - WS-F6700-DFC3CXL
  - WS-F6700-DFC3C
  - WS-F6700-DFC3BXL (not supported in virtual switch mode)
  - WS-F6700-DFC3B (not supported in virtual switch mode)
  - WS-F6700-DFC3A (not supported in virtual switch mode)
  - WS-F6700-CFC
- WS-X6704-10GE ships with WS-F6700-CFC installed unless ordered with WS-F6700-DFC3CXL, WS-F6700-DFC3C, WS-F6700-DFC3BXL, WS-F6700-DFC3B, or WS-F6700-DFC3A.
- WS-X6704-10GE is supported in the WS-C6503-E chassis.
- WS-X6704-10GE is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6704-10GE is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6704-10GE ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6704-10GE ports that interconnect network devices.
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html
- Does not support ISL encapsulation.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6704-10GE** | 4-port 10-Gigabit Ethernet XENPAK<br>• dCEF720 with a DFC<br>• CEF720 with WS-F6700-CFC<br>• Supports egress multicast replication<br>• QoS port architecture (Rx/Tx):<br>– With DFC3: **8q8t/1p7q8t**<br>– With CFC: **1q8t/1p7q8t**<br>• Dual switch-fabric connections<br>Fabric Channel #1: Ports 3 and 4<br>Fabric Channel #2: Ports 1 and 2<br>• Number of ports: 4<br>Number of port groups: 4<br>Port ranges per port group: 1 port in each group | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 and DFC3C or DFC3CXL | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17a)SX |

## WS-X6502-10GE 1-port 10-Gigabit Ethernet Switching Module

**Note**

- WS-X6502-10GE does not support ISL encapsulation.
- Use with Release 12.2(33)SXH or later and a DFC requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6010.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-X6502-10GE** | 1-port 10-Gigabit Ethernet<br>• dCEF256 with a DFC<br>• QoS port architecture (Rx/Tx): **1p1q8t/1p2q1t**<br>• Number of ports: 1<br>Number of port groups: 1<br>Port ranges per port group: 1 port in 1 group | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **Optical Interface Module (OIM) for WS-X6502-10GE** | | |
| **WS-G6488** | 10GBASE-LR serial 1310 nm long-reach OIM | 12.2(14)SX |
| **WS-G6483** | 10GBASE-ER serial 1550 nm extended-reach OIM | 12.2(14)SX |

# Gigabit Ethernet Switching Modules


- WS-X6748-SFP 48-port Gigabit Ethernet SFP Switching Module, page 51
- WS-X6724-SFP 24-port Gigabit Ethernet SFP Switching Module, page 53
- WS-X6816-GBIC 16-port Gigabit Ethernet GBIC Switching Module, page 55
- WS-X6516A-GBIC 16-Port Gigabit Ethernet GBIC Switching Module, page 56
- WS-X6516-GBIC 16-Port Gigabit Ethernet GBIC Switching Module, page 57
- WS-X6416-GBIC 16-port Gigabit Ethernet GBIC Switching Module, page 58
- WS-X6408A-GBIC 8-port Gigabit Ethernet GBIC Switching Module, page 58
- WS-X6408-GBIC 8-port Gigabit Ethernet GBIC Switching Module, page 59


## WS-X6748-SFP 48-port Gigabit Ethernet SFP Switching Module

**Note**

- WS-X6748-SFP requires one of the following:
  - WS-F6700-DFC3CXL
  - WS-F6700-DFC3C
  - WS-F6700-DFC3BXL
  - WS-F6700-DFC3B
  - WS-F6700-DFC3A
  - WS-F6700-CFC
- WS-X6748-SFP ships with WS-F6700-CFC installed unless ordered with WS-F6700-DFC3CXL, WS-F6700-DFC3C, WS-F6700-DFC3BXL, WS-F6700-DFC3B, or WS-F6700-DFC3A.
- WS-X6748-SFP is supported in the WS-C6503-E chassis.
- WS-X6748-SFP is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6748-SFP is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6748-SFP ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6748-SFP ports that interconnect network devices.
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6748-SFP** | 48-port Gigabit Ethernet SFP<br>• dCEF720 with a DFC (only WS-F6700-DFC3CXL and WS-F6700-DFC3C are supported in virtual switch mode)<br>• CEF720 with WS-F6700-CFC<br>• Supports egress multicast replication<br>• QoS architecture:<br>– With DFC3: **2q8t/1p3q8t**<br>– With CFC: **1q8t/1p3q8t**<br>• Dual switch-fabric connections<br>Fabric Channel #1: Ports 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48<br>Fabric Channel #2: Ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47<br>• Number of ports: 48<br>Number of port groups: 4<br>Port ranges per port group:<br>1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23<br>2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24<br>25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47<br>26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 and DFC3C or DFC3CXL | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17d)SXB |

## WS-X6724-SFP 24-port Gigabit Ethernet SFP Switching Module

**Note**

- WS-X6724-SFP requires one of the following:
  - WS-F6700-DFC3CXL
  - WS-F6700-DFC3C
  - WS-F6700-DFC3BXL (not supported in virtual switch mode)
  - WS-F6700-DFC3B (not supported in virtual switch mode)
  - WS-F6700-DFC3A (not supported in virtual switch mode)
  - WS-F6700-CFC
- WS-X6724-SFP ships with WS-F6700-CFC installed unless ordered with WS-F6700-DFC3CXL, WS-F6700-DFC3C, WS-F6700-DFC3BXL, WS-F6700-DFC3B, or WS-F6700-DFC3A.
- WS-X6724-SFP is supported in the WS-C6503-E chassis.
- WS-X6724-SFP is not supported in the WS-C6503 and CISCO7603 chassis.
- WS-X6724-SFP is supported in all slots of a 13-slot chassis.
- On WS-X6724-SFP ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6724-SFP ports that interconnect network devices.
- Use with Release 12.2(33)SXH or later requires switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6724-SFP** | 24-port Gigabit Mbps Ethernet SFP<br>• dCEF720 with a DFC<br>• CEF720 with WS-F6700-CFC<br>• Supports egress multicast replication<br>• QoS architecture:<br>– With DFC3: **2q8t/1p3q8t**<br>– With CFC: **1q8t/1p3q8t**<br>• Number of ports: 24<br>Number of port groups: 2<br>Port ranges per port group: 1–12, 13–24 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 and DFC3C or DFC3CXL | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17a)SX |

## WS-X6816-GBIC 16-port Gigabit Ethernet GBIC Switching Module

**Note**

- WS-X6816-GBIC requires one of these for use with Supervisor Engine 720-10GE or Supervisor Engine 720:
  - WS-F6K-DFC3BXL
  - WS-F6K-DFC3B
  - WS-F6K-DFC3A
- In a 13-slot chassis, WS-X6816-GBIC is supported only in slots 9 through 13 and does not power up in other slots.
- Use with Release 12.2(33)SXH or later requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6010.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-X6816-GBIC** | 16-port Gigabit Ethernet GBIC<br>• dCEF256<br>• QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**<br>• Dual switch-fabric connections<br>Fabric Channel #1: Ports 1–8<br>Fabric Channel #2: Ports 9–16<br>• Number of ports: 16<br>Number of port groups: 2<br>Port ranges per port group: 1–8, 9–16 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |

## WS-X6516A-GBIC 16-Port Gigabit Ethernet GBIC Switching Module

**Note**

- Use with Release 12.2(33)SXH or later requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6010.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-X6516A-GBIC** | 16-port Gigabit Ethernet GBIC<br>• dCEF256 with a DFC<br>• CEF256<br>• 1-MB per-port packet buffers<br>• Supports egress multicast replication<br>• QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**<br>• Number of ports: 16<br>Number of port groups: 2<br>Port ranges per port group: 1–8, 9–16 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6516-GBIC 16-Port Gigabit Ethernet GBIC Switching Module

**Note**

- Use with Release 12.2(33)SXH or later and a DFC requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6010.html

- Supervisor Engine 720 supports a DFC3 on these WS-X6516-GBIC hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-X6516-GBIC** | 16-port Gigabit Ethernet GBIC<br>• dCEF256 with a DFC<br>• CEF256<br>• 512-KB per-port packet buffers<br>• QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**<br>• Number of ports: 16<br>Number of port groups: 2<br>Port ranges per port group: 1–8, 9–16 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6416-GBIC 16-port Gigabit Ethernet GBIC Switching Module

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6416-GBIC** | 16-port Gigabit Ethernet GBIC<br>• QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**<br>• Number of ports: 16<br>Number of port groups: 2<br>Port ranges per port group: 1–8, 9–16 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6408A-GBIC 8-port Gigabit Ethernet GBIC Switching Module

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6408A-GBIC** | 8-port Gigabit Ethernet GBIC<br>• QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**<br>• Number of ports: 8<br>Number of port groups: 1<br>Port ranges per port group: 1–8 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

### WS-X6408-GBIC 8-port Gigabit Ethernet GBIC Switching Module

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6408-GBIC** | 8-port Gigabit Ethernet GBIC<br>• QoS port architecture (Rx/Tx): **1q4t/2q2t**<br>• Number of ports: 8<br>Number of port groups: 1<br>Port ranges per port group: 1–8 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## 10/100/1000 Ethernet Switching Modules


- WS-X6748-GE-TX, page 60
- WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF, page 61
- WS-X6148E-GE-45AT, page 63
- WS-X6148A-GE-TX, WS-X6148A-GE-45AF, page 64
- WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, page 65
- WS-X6516-GE-TX, page 66

## WS-X6748-GE-TX

**Note**

- WS-X6748-GE-TX requires one of the following:
  - WS-F6700-DFC3CXL
  - WS-F6700-DFC3C
  - WS-F6700-DFC3BXL (not supported in virtual switch mode)
  - WS-F6700-DFC3B (not supported in virtual switch mode)
  - WS-F6700-DFC3A (not supported in virtual switch mode)
  - WS-F6700-CFC
- WS-X6748-GE-TX ships with WS-F6700-CFC installed unless ordered with WS-F6700-DFC3CXL, WS-F6700-DFC3C, WS-F6700-DFC3BXL, WS-F6700-DFC3B, or WS-F6700-DFC3A.
- WS-X6748-GE-TX is supported in the WS-C6503-E chassis.
- WS-X6748-GE-TX is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6748-GE-TX is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6748-GE-TX ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6748-GE-TX ports that interconnect network devices.
- Use with Release 12.2(33)SXH or later and a DFC requires DFC ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6010.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6748-GE-TX** | 48-port 10/100/1000 RJ-45<br>• dCEF720 with a DFC<br>• CEF720 with WS-F6700-CFC<br>• Supports egress multicast replication<br>• QoS architecture:<br>– With DFC3: **2q8t/1p3q8t**<br>– With CFC: **1q8t/1p3q8t**<br>• Dual switch-fabric connections<br>Fabric Channel #1: Ports 25–48<br>Fabric Channel #2: Ports 1–24<br>• Number of ports: 48<br>Number of port groups: 4<br>Port ranges per port group: 1–12, 13–24, 25–36, 37–48 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17a)SX |

## WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548-GE-45AF

**Note**

- Release 12.2(17b)SXA and later releases provide support for more than 1 Gbps of traffic per EtherChannel on the WS-X6548-GE-TX (and voice-power daughtercard equipped) switching modules.
- WS-X6548-GE-TX (and voice-power daughtercard equipped) switching modules do not support these features:
  - DFCs
  - ISL trunking
  - Jumbo frames
  - 802.1Q tunneling
  - Traffic storm control

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6548-GE-TX**<br>**WS-X6548V-GE-TX**<br>**WS-X6548-GE-45AF** | 48-port 10/100/1000 Mbps<br>• RJ-45<br>• CEF256<br>• WS-X6548-GE-TX supports:<br>– WS-F6K-VPWR-GE<br>– WS-F6K-GE48-AF<br>– WS-F6K-48-AF<br>• WS-X6548V-GE-TX has WS-F6K-VPWR-GE<br>• WS-X6548-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF<br>• With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W).<br>• QoS port architecture (Rx/Tx): **1q2t/1p2q2t**<br>• Number of ports: 48<br>Number of port groups: 2<br>Port ranges per port group: 1–24, 25–48<br>• The aggregate bandwidth of each set of 8 ports (1–8, 9–16, 17–24, 25–32, 33–40, and 41–48) is 1 Gbps. | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720<br>(except WS-F6K-GE48-AF or WS-F6K-48-AF) | 12.2(17a)SX |
| | WS-F6K-GE48-AF or WS-F6K-48-AF<br>with Supervisor Engine 720 | 12.2(17d)SXB |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| | WS-F6K-GE48-AF or WS-F6K-48-AF<br>with Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6148E-GE-45AT

**Note**

- WS-X6148E-GE-45AT does not support:
  - DFC
  - Traffic storm control

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6148E-GE-45AT** | 48-port 10/100/1000 Mbps<br>• RJ-45<br>• WS-X6148E-GE-45AT has WS-F6K-48-AT (IEEE 802.3at PoE)<br>– With Release 12.2(33)SXJ2 and later releases, supports Class 4 PoE+: 30.00 W at the PSE (12.95 W to 25.50 W at the PD).<br>– With Releases earlier than Release 12.2(33)SXJ2, supports up to 45 ports of ePoE (16.8 W at the PSE, ePoE for 45 ports maximum).<br>• QoS port architecture (Rx/Tx): **1q2t/1p3q8t**<br>• Number of ports: 48<br>Number of port groups: 6<br>Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48<br>• The aggregate bandwidth of each set of 8 ports (1–8, 9–16, 17–24, 25–32, 33–40, and 41–48) is 1 Gbps. | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXI4 |
| | With Supervisor Engine 720 | |
| | With Supervisor Engine 32 | |

## WS-X6148A-GE-TX, WS-X6148A-GE-45AF

**Note**

- WS-X6148A-GE-TX and WS-X6148A-GE-45AF do not support these features:
  - WS-F6K-DFC3A, WS-F6K-DFC3B, or WS-F6K-DFC3BXL
  - Traffic storm control

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-X6148A-GE-TX**<br>**WS-X6148A-GE-45AF** | 48-port 10/100/1000 Mbps<br>• RJ-45<br>• WS-X6148A-GE-TX supports WS-F6K-GE48-AF or WS-F6K-48-AF<br>• WS-X6148A-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF<br>• With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W).<br>• QoS port architecture (Rx/Tx): **1q2t/1p3q8t**<br>• Number of ports: 48<br>Number of port groups: 6<br>Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48<br>• The aggregate bandwidth of each set of 8 ports (1–8, 9–16, 17–24, 25–32, 33–40, and 41–48) is 1 Gbps. | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF

**Note**

- WS-X6148-GE-TX, WS-X6148V-GE-TX, and WS-X6148-GE-45AF do not support these features:
  - More than 1 Gbps of traffic per EtherChannel
  - WS-F6K-DFC3A, WS-F6K-DFC3B, or WS-F6K-DFC3BXL
  - ISL trunking
  - Jumbo frames
  - 802.1Q tunneling
  - Traffic storm control

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-X6148-GE-TX**<br>**WS-X6148V-GE-TX**<br>**WS-X6148-GE-45AF** | 48-port 10/100/1000 Mbps<br>• RJ-45<br>• WS-X6148-GE-TX supports:<br>– WS-F6K-VPWR-GE<br>– WS-F6K-GE48-AF<br>– WS-F6K-48-AF<br>• WS-X6148V-GE-TX has WS-F6K-VPWR-GE<br>• WS-X6148-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF<br>• With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W).<br>• QoS port architecture (Rx/Tx): **1q2t/1p2q2t**<br>• Number of ports: 48<br>Number of port groups: 2<br>Port ranges per port group: 1–24, 25–48<br>• The aggregate bandwidth of each port group is 1 Gbps. | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720<br>(except WS-F6K-GE48-AF or WS-F6K-48-AF) | 12.2(17a)SX |
| | WS-F6K-GE48-AF or WS-F6K-48-AF<br>with Supervisor Engine 720 | 12.2(17d)SXB |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| | WS-F6K-GE48-AF or WS-F6K-48-AF<br>with Supervisor Engine 32 | 12.2(18)SXF |

### WS-X6516-GE-TX

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6516-GE-TX** | 16-port 10/100/1000BASE-T<br>• dCEF256 with a DFC<br>• CEF256<br>• QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**<br>• Number of ports: 16<br>Number of port groups: 2<br>Port ranges per port group: 1–8, 9–16 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## Fast Ethernet Switching Modules


- WS-X6148-FE-SFP, page 66
- WS-X6524-100FX-MM, page 67
- WS-X6324-100FX-MM, page 67


**Note** Fast Ethernet switching modules are not supported in VSS mode.

### WS-X6148-FE-SFP

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6148-FE-SFP** | 48-port 100BASE-FX<br>• Requires Fast Ethernet SFPs<br>• QoS port architecture (Rx/Tx): **1p1q4t/1p3q8t**<br>• Number of ports: 48<br>Number of port groups: 3<br>Port ranges per port group: 1–16, 17–32, and 33–48 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6524-100FX-MM

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6524-100FX-MM** | 24-port 100FX Ethernet multimode<br>• dCEF256 with a DFC<br>• CEF256<br>• QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**<br>• Number of ports: 24<br>Number of port groups: 1<br>Port ranges per port group: 1–24 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6324-100FX-MM

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6324-100FX-MM** | 24-port 100FX Ethernet<br>• Single mode and multimode MT-RJ<br>• 128-KB per-port packet buffers<br>• QoS port architecture (Rx/Tx): **1q4t/2q2t**<br>• Number of ports: 24<br>Number of port groups: 2<br>Port ranges per port group: 1–12, 13–24 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

# Ethernet/Fast Ethernet (10/100) Switching Modules


- WS-X6548-RJ-45, page 68
- WS-X6548-RJ-21, page 69
- WS-X6148X2-RJ-45, WS-X6148X2-45AF, page 69
- WS-X6196-RJ-21, WS-X6196-21AF, page 70
- WS-X6348-RJ-45, WS-X6348-RJ-45V, page 70
- WS-X6348-RJ-21V, page 71
- WS-X6148A-RJ-45, WS-X6148A-45AF, page 71
- WS-X6148-RJ-45, WS-X6148-RJ45V, WS-X6148-45AF, page 72
- WS-X6148-RJ-21, WS-X6148-RJ21V, WS-X6148-21AF, page 73
- WS-F6K-FE48X2-AF, page 74
- WS-F6K-GE48-AF, WS-F6K-48-AF, page 74
- WS-F6K-GE48-AF, WS-F6K-48-AF, page 74


**Note** Ethernet/Fast Ethernet (10/100) switching modules are not supported in VSS mode.

## WS-X6548-RJ-45

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-X6548-RJ-45** | 48-port 10/100TX RJ-45<br>• dCEF256 with a DFC<br>• CEF256<br>• QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**<br>• Number of ports: 48<br>Number of port groups: 1<br>Port ranges per port group: 1–48 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6548-RJ-21

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6548-RJ-21** | 48-port 10/100TX RJ-21<br>• dCEF256 with a DFC<br>• CEF256<br>• QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**<br>• Number of ports: 48<br>Number of port groups: 1<br>Port ranges per port group: 1–48 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6148X2-RJ-45, WS-X6148X2-45AF

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6148X2-RJ-45**<br>**WS-X6148X2-45AF** | 96-port 10/100TX RJ-45<br>• QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**<br>• WS-X6148X2-RJ-45 supports WS-F6K-FE48X2-AF<br>• WS-X6148X2-45AF has WS-F6K-FE48X2-AF | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF3 |
| | With Supervisor Engine 32 | 12.2(18)SXF3 |

## WS-X6196-RJ-21, WS-X6196-21AF

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6196-RJ-21**<br>**WS-X6196-21AF** | 96-port 10/100TX RJ-21<br>• QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**<br>• WS-X6196-RJ-21 supports WS-F6K-FE48X2-AF<br>• WS-X6196-21AF has WS-F6K-FE48X2-AF | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF3 |
| | With Supervisor Engine 32 | 12.2(18)SXF3 |

## WS-X6348-RJ-45, WS-X6348-RJ-45V

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6348-RJ-45**<br>**WS-X6348-RJ-45V** | 48-port 10/100TX RJ-45<br>• 128-KB per-port packet buffers<br>• QoS port architecture (Rx/Tx): **1q4t/2q2t**<br>• WS-X6348-RJ-45 supports WS-F6K-VPWR<br>• WS-X6348-RJ-45V has WS-F6K-VPWR<br>• Number of ports: 48<br>Number of port groups: 4<br>Port ranges per port group: 1–12, 13–24, 25–36, 37–48 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6348-RJ-21V

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6348-RJ-21V** | 48-port 10/100TX RJ-21<br>• 128-KB per-port packet buffers<br>• QoS port architecture (Rx/Tx): **1q4t/2q2t**<br>• Has WS-F6K-VPWR<br>• Number of ports: 48<br>Number of port groups: 4<br>Port ranges per port group: 1–12, 13–24, 25–36, 37–48 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6148A-RJ-45, WS-X6148A-45AF

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6148A-RJ-45**<br>**WS-X6148A-45AF** | 48-port 10/100TX RJ-45<br>• 5.3-MB per-port packet buffers<br>• QoS port architecture (Rx/Tx): **1p1q4t/1p3q8t**<br>• WS-X6148A-RJ-45 supports WS-F6K-GE48-AF or WS-F6K-48-AF<br>• WS-X6148A-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF<br>• Number of ports: 48<br>Number of port groups: 6<br>Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-X6148-RJ-45, WS-X6148-RJ45V, WS-X6148-45AF

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6148-RJ-45**<br>**WS-X6148-RJ45V**<br>**WS-X6148-45AF** | 48-port 10/100TX RJ-45<br>• 128-KB per-port packet buffers<br>• QoS port architecture (Rx/Tx): **1q4t/2q2t**<br>• WS-X6148-RJ-45 supports WS-F6K-VPWR<br>• WS-X6148-RJ-45V has WS-F6K-VPWR<br>• WS-X6148-45AF has WS-F6K-48-AF<br>• Number of ports: 48<br>Number of port groups: 4<br>Port ranges per port group: 1–12, 13–24, 25–36, 37–48 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 (except with WS-F6K-48-AF) | 12.2(14)SX |
| | WS-F6K-48-AF with Supervisor Engine 720 | 12.2(17d)SXB |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| | WS-F6K-48-AF with Supervisor Engine 32 | |

## WS-X6148-RJ-21, WS-X6148-RJ21V, WS-X6148-21AF

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6148-RJ-21**<br>**WS-X6148-RJ21V**<br>**WS-X6148-21AF** | 48-port 10/100TX RJ-21<br>• 128-KB per-port packet buffers<br>• QoS port architecture (Rx/Tx): **1q4t/2q2t**<br>• WS-X6148-RJ-21 supports WS-F6K-VPWR<br>• WS-X6148-RJ-21V has WS-F6K-VPWR<br>• WS-X6148-21AF has WS-F6K-48-AF<br>• Number of ports: 48<br>Number of port groups: 4<br>Port ranges per port group: 1–12, 13–24, 25–36, 37–48 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 (except with WS-F6K-48-AF) | 12.2(14)SX |
| | WS-F6K-48-AF with Supervisor Engine 720 | 12.2(17d)SXB |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| | WS-F6K-48-AF with Supervisor Engine 32 | |

# Power over Ethernet Daughtercards

**Note** The IEEE 802.3at power over ethernet (PoE) daughtercard is available only with the WS-X6148E-GE-45AT switching module.


- WS-F6K-FE48X2-AF, page 74
- WS-F6K-GE48-AF, WS-F6K-48-AF, page 74
- WS-F6K-VPWR-GE, page 75
- WS-F6K-VPWR, page 75

## WS-F6K-FE48X2-AF

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-F6K-FE48X2-AF** | IEEE 802.3af PoE daughtercard for WS-X6148X2-RJ-45 and WS-X6196-RJ-21. | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-F6K-GE48-AF, WS-F6K-48-AF

**Note**

- WS-F6K-GE48-AF and WS-F6K-48-AF are not FRUs for these switching modules:
  - WS-X6148-RJ-45 or WS-X6148-RJ-45V (replace with WS-X6148-45AF-UG=).
  - WS-X6148-RJ-21 or WS-X6148-RJ-21V (replace with WS-X6148-21AF-UG=).
- With WS-X6548-GE-TX, WS-X6148-GE-TX, and WS-X6148A-GE-TX, supports up to 45 ports of ePoE (16.8W).

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-F6K-GE48-AF**<br>**WS-F6K-48-AF** | IEEE 802.3af PoE daughtercard for:<br>• WS-X6548-GE-TX<br>• WS-X6148-GE-TX<br>• WS-X6148A-GE-TX<br>• WS-X6148A-RJ-45 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17d)SXB |

## WS-F6K-VPWR-GE

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-F6K-VPWR-GE** | Prestandard PoE daughtercard for WS-X6548-GE-TX and WS-X6148-GE-TX | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17a)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## WS-F6K-VPWR

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-F6K-VPWR** | Prestandard PoE daughtercard for:<br>• WS-X6348-RJ-45<br>• WS-X6348-RJ-21V<br>• WS-X6148-RJ-45<br>• WS-X6148-RJ-21 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

# Transceivers


- X2 Modules, page 76
- XENPAKs, page 78
- Small Form-Factor Pluggable (SFP) Modules, page 80
- Gigabit Interface Converters (GBICs), page 82

## X2 Modules

**Note**

- WS-X6708-10GE and WS-X6716-10G do not support X2 modules shipped before the release of WS-X6708-10GE with Release 12.2(18)SXF5. The unsupported X2 modules are labeled with a number that ends with -01. (This restriction does not apply to X2-10GB-LRM.)
- All X2 modules shipped since WS-X6716-10G became available provide EMI compliance with WS-X6716-10G.
- Some X2 modules shipped before WS-X6716-10G became available might not provide EMI compliance with WS-X6716-10G. See the information listed for each type of X2 module in the following table.
- For information about X2 modules, see the *Cisco 10GBASE X2 Modules* data sheet:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6574/product_data_sheet0900aecd801f92aa.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **CVR-X2-SFP10G** | 10G X2 to SFP+ Converter | 12.2(33)SXI2 |
| | **10 Gbps Ethernet SFP+ Modules** | |
| | SFP-10G-LR—10GBASE-LR 1310 nm SMF | 12.2(33)SXJ1 |
| | SFP-10G-LRM—10GBASE-LRM 1310 nm MMF and SMF | 12.2(33)SXI4<br>(12.2(33)SXI4a or later recommended) |
| | SFP-10G-SR—10GBASE-SR 850 nm MMF | 12.2(33)SXI2 |
| | SFP-H10GB-CU1M—1m Twinax cable, passive, 30AWG cable assembly | |
| | SFP-H10GB-CU3M—3m Twinax cable, passive, 30AWG cable assembly | |
| | SFP-H10GB-CU5M—5m Twinax cable, passive, 24AWG cable assembly | |

| Product ID (append "=" for spares) | Product Description | | Minimum Software Versions |
|---|---|---|---|
| **DWDM-X2-60.61=** | 10GBASE-DWDM 1560.61 nm X2 (100-GHz ITU grid) | ITU 21 | 12.2(33)SXI |
| **DWDM-X2-59.79=** | 10GBASE-DWDM 1559.79 nm X2 (100-GHz ITU grid) | ITU 22 | |
| **DWDM-X2-58.98=** | 10GBASE-DWDM 1558.98 nm X2 (100-GHz ITU grid) | ITU 23 | |
| **DWDM-X2-58.17=** | 10GBASE-DWDM 1558.17 nm X2 (100-GHz ITU grid) | ITU 24 | |
| **DWDM-X2-56.55=** | 10GBASE-DWDM 1556.55 nm X2 (100-GHz ITU grid) | ITU 26 | |
| **DWDM-X2-55.75=** | 10GBASE-DWDM 1555.75 nm X2 (100-GHz ITU grid) | ITU 27 | |
| **DWDM-X2-54.94=** | 10GBASE-DWDM 1554.94 nm X2 (100-GHz ITU grid) | ITU 28 | |
| **DWDM-X2-54.13=** | 10GBASE-DWDM 1554.13 nm X2 (100-GHz ITU grid) | ITU 29 | |
| **DWDM-X2-52.52=** | 10GBASE-DWDM 1552.52 nm X2 (100-GHz ITU grid) | ITU 31 | |
| **DWDM-X2-51.72=** | 10GBASE-DWDM 1551.72 nm X2 (100-GHz ITU grid) | ITU 32 | |
| **DWDM-X2-50.92=** | 10GBASE-DWDM 1550.92 nm X2 (100-GHz ITU grid) | ITU 33 | |
| **DWDM-X2-50.12=** | 10GBASE-DWDM 1550.12 nm X2 (100-GHz ITU grid) | ITU 34 | |
| **DWDM-X2-48.51=** | 10GBASE-DWDM 1548.51 nm X2 (100-GHz ITU grid) | ITU 36 | |
| **DWDM-X2-47.72=** | 10GBASE-DWDM 1547.72 nm X2 (100-GHz ITU grid) | ITU 37 | |
| **DWDM-X2-46.92=** | 10GBASE-DWDM 1546.92 nm X2 (100-GHz ITU grid) | ITU 38 | |
| **DWDM-X2-46.12=** | 10GBASE-DWDM 1546.12 nm X2 (100-GHz ITU grid) | ITU 39 | |
| **DWDM-X2-44.53=** | 10GBASE-DWDM 1544.53 nm X2 (100-GHz ITU grid) | ITU 41 | |
| **DWDM-X2-43.73=** | 10GBASE-DWDM 1543.73 nm X2 (100-GHz ITU grid) | ITU 42 | |
| **DWDM-X2-42.94=** | 10GBASE-DWDM 1542.94 nm X2 (100-GHz ITU grid) | ITU 43 | |
| **DWDM-X2-42.14=** | 10GBASE-DWDM 1542.14 nm X2 (100-GHz ITU grid) | ITU 44 | |
| **DWDM-X2-40.56=** | 10GBASE-DWDM 1540.56 nm X2 (100-GHz ITU grid) | ITU 46 | |
| **DWDM-X2-39.77=** | 10GBASE-DWDM 1539.77 nm X2 (100-GHz ITU grid) | ITU 47 | |
| **DWDM-X2-38.98=** | 10GBASE-DWDM 1538.98 nm X2 (100-GHz ITU grid) | ITU 48 | |
| **DWDM-X2-38.19=** | 10GBASE-DWDM 1538.19 nm X2 (100-GHz ITU grid) | ITU 49 | |
| **DWDM-X2-36.61=** | 10GBASE-DWDM 1536.61 nm X2 (100-GHz ITU grid) | ITU 51 | |
| **DWDM-X2-35.82=** | 10GBASE-DWDM 1535.82 nm X2 (100-GHz ITU grid) | ITU 52 | |
| **DWDM-X2-35.04=** | 10GBASE-DWDM 1535.04 nm X2 (100-GHz ITU grid) | ITU 53 | |
| **DWDM-X2-34.25=** | 10GBASE-DWDM 1534.25 nm X2 (100-GHz ITU grid) | ITU 54 | |
| **DWDM-X2-32.68=** | 10GBASE-DWDM 1532.68 nm X2 (100-GHz ITU grid) | ITU 56 | |
| **DWDM-X2-31.90=** | 10GBASE-DWDM 1531.90 nm X2 (100-GHz ITU grid) | ITU 57 | |
| **DWDM-X2-31.12=** | 10GBASE-DWDM 1531.12 nm X2 (100-GHz ITU grid) | ITU 58 | |
| **DWDM-X2-30.33=** | 10GBASE-DWDM 1530.33 nm X2 (100-GHz ITU grid) | ITU 59 | |
| **X2-10GB-T** | 10GBASE-T X2 Module for CAT6A/CAT7 copper cable | | 12.2(33)SXJ1 |
| **X2-10GB-ZR** | 10GBASE-ZR X2 Module for SMF | | 12.2(33)SXI |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **X2-10GB-CX4** | 10GBASE for CX4 (copper) cable | 12.2(18)SXF5 |
| **X2-10GB-ER** | 10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)<br>**Note** X2-10GB-ER modules labeled with a number that ends with -02 do not provide EMI compliance with WS-X6716-10G. | 12.2(18)SXF5 |
| **X2-10GB-LR** | 10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)<br>**Note** X2-10GB-LR modules labeled with a number that ends with -02 or -03 do not provide EMI compliance with WS-X6716-10G. | 12.2(18)SXF5 |
| **X2-10GB-LRM** | 10GBASE-LRM for FDDI-grade multimode fiber (MMF)<br>**Note** Not supported by the **show idprom** command. (CSCsj35671) | 12.2(18)SXF8 |
| **X2-10GB-LX4** | 10GBASE-LX4 Serial 1310-nm multimode (MMF)<br>**Note**<br>• See field notice 62840 for information about unsupported 10GBASE-LX4 modules:<br>http://www.cisco.com/en/US/ts/fn/misc/FN62840.html<br>• X2-10GB-LX4 modules labeled with a number that ends with -01 to -03 do not provide EMI compliance with WS-X6716-10G. | 12.2(18)SXF5 |
| **X2-10GB-SR** | 10GBASE-SR Serial 850-nm short-reach multimode (MMF) | 12.2(18)SXF5 |

## XENPAKs

**Note**

- For information about DWDM XENPAKs, see the *Cisco 10GBase DWDM XENPAK Modules* data sheet:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6576/product_data_sheet0900aecd801f9333.html

- For information about other XENPAKs, see the *Cisco 10GBASE XENPAK Modules* data sheet:

  http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a008007cd00_ps5251_Products_Data_Sheet.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **XENPAK-10GB-LRM** | 10GBASE-LRM XENPAK Module for MMF<br>**Note** Not supported by the **show idprom** command. (CSCsl21260) | 12.2(33)SXH1 |
| **DWDM-XENPAK** | 10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid | 12.2(18)SXE |
| **WDM-XENPAK-REC** | 10GBASE receive-only wavelength division multiplexing (WDM) | 12.2(18)SXE |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **XENPAK-10GB-CX4** | 10GBASE for CX4 (copper) cable; uses Infiniband connectors | 12.2(17d)SXB1 |
| **XENPAK-10GB-ER** | 10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)<br>**Note** XENPAK-10GB-ER units with Part No. 800-24557-01 are not supported, as described in this external field notice (CSCee47030):<br>http://www.cisco.com/en/US/ts/fn/200/fn29736.html | 12.2(17a)SX |
| **XENPAK-10GB-ER+** | 10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) | 12.2(17a)SX |
| **XENPAK-10GB-LR** | 10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) | 12.2(17a)SX |
| **XENPAK-10GB-LR+** | 10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) | 12.2(17a)SX |
| **XENPAK-10GB-LW** | 10GBASE-LW XENPAK Module with WAN PHY for SMF<br>**Note** XENPAK-10GB-LW operates at an interface speed compatible with SONET/SDH OC-192/STM-64. XENPAK-10GB-LW links might go up and down if the data rate exceeds 9Gbs. (CSCsi58211) | 12.2(18)SXE |
| **XENPAK-10GB-LX4** | 10GBASE-LX4 Serial 1310-nm multimode (MMF) | 12.2(17a)SX1 |
| **XENPAK-10GB-SR** | 10GBASE-SR Serial 850-nm short-reach multimode (MMF) | 12.2(17a)SX1 |
| **XENPAK-10GB-ZR** | 10GBASE for any SMF type | 12.2(18)SXF |

## Small Form-Factor Pluggable (SFP) Modules

These sections describe SFPs:


- 10 Gbps Ethernet SFP+ Modules, page 76
- Gigabit Ethernet SFP Modules, page 80
- Fast Ethernet SFP+ Modules, page 82


### Gigabit Ethernet SFP Modules

**Note**

- For information about coarse wavelength-division multiplexing (CWDM) SFPs, see the *Cisco CWDM GBIC and SFP Solutions* data sheet:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6575/product_data_sheet09186a00801a557c_ps4999_Products_Data_Sheet.html

- For information about DWDM SFPs, see the *Cisco Dense Wavelength-Division Multiplexing Small Form-Factor Pluggable Module* data sheet:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6576/product_data_sheet0900aecd80582763.html

- See the "Unsupported Hardware" section on page 112 for information about unsupported DWDM-SFPs.

- For information about other SFPs, see the *Cisco SFP Optics For Gigabit Ethernet Applications* data sheet:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6577/product_data_sheet0900aecd8033f885.html

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **GLC-BX-D** | 1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength | 12.2(18)SXE |
| **GLC-BX-U** | 1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength | 12.2(18)SXE |
| **GLC-LH-SMD**<br>**GLC-LH-SM** | 1000BASE-LX/LH SFP | 12.2(17a)SX |
| **GLC-SX-MMD**<br>**GLC-SX-MM** | 1000BASE-SX SFP | 12.2(14)SX |
| **GLC-T** | 1000BASE-T 10/100/1000 SFP module<br>**Note** Supported only at 1000 Mbps. | 12.2(17a)SX |
| **GLC-ZX-SM** | 1000BASE-ZX SFP module | 12.2(17d)SXB1 |
| **CWDM-SFP-1470** | CWDM 1470-nm (Gray) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module | 12.2(17a)SX |
| **CWDM-SFP-1490** | CWDM 1490-nm (Violet) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module | 12.2(17a)SX |
| **CWDM-SFP-1510** | CWDM 1510-nm (Blue) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module | 12.2(17a)SX |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **CWDM-SFP-1530** | CWDM 1530-nm (Green) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module | 12.2(17a)SX |
| **CWDM-SFP-1550** | CWDM 1550-nm (Yellow) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module | 12.2(17a)SX |
| **CWDM-SFP-1570** | CWDM 1570-nm (Orange) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module | 12.2(17a)SX |
| **CWDM-SFP-1590** | CWDM 1590-nm (Red) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module | 12.2(17a)SX |
| **CWDM-SFP-1610** | CWDM 1610-nm (Brown) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module | 12.2(17a)SX |
| **DWDM-SFP-5817** | 1000BASE-DWDM 1558.17 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-5252** | 1000BASE-DWDM 1552.52 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-5172** | 1000BASE-DWDM 1551.72 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-5012** | 1000BASE-DWDM 1550.12 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-4692** | 1000BASE-DWDM 1546.92 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-4373** | 1000BASE-DWDM 1543.73 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-4214** | 1000BASE-DWDM 1542.14 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-3977** | 1000BASE-DWDM 1539.77 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-3898** | 1000BASE-DWDM 1538.98 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-3582** | 1000BASE-DWDM 1535.82 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-3504** | 1000BASE-DWDM 1535.04 nm SFP (100-GHz ITU grid) SFP module | 12.2(33)SXH |
| **DWDM-SFP-6061** | 1000BASE-DWDM 1560.61 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-5979** | 1000BASE-DWDM 1559.79 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-5898** | 1000BASE-DWDM 1558.98 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-5655** | 1000BASE-DWDM 1556.55 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-5575** | 1000BASE-DWDM 1555.75 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-5494** | 1000BASE-DWDM 1554.94 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-5413** | 1000BASE-DWDM 1554.13 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-5092** | 1000BASE-DWDM 1550.92 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-4851** | 1000BASE-DWDM 1548.51 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-4772** | 1000BASE-DWDM 1547.72 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-4612** | 1000BASE-DWDM 1546.12 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-4453** | 1000BASE-DWDM 1544.53 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-4294** | 1000BASE-DWDM 1542.94 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-4056** | 1000BASE-DWDM 1540.56 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-3819** | 1000BASE-DWDM 1538.19 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-3661** | 1000BASE-DWDM 1536.61 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-3425** | 1000BASE-DWDM 1534.25 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-3268** | 1000BASE-DWDM 1532.68 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **DWDM-SFP-3190** | 1000BASE-DWDM 1531.90 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-3112** | 1000BASE-DWDM 1531.12 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |
| **DWDM-SFP-3033** | 1000BASE-DWDM 1530.33 nm SFP (100-GHz ITU grid) SFP module | 12.2(18)SXF8 |

### Fast Ethernet SFP+ Modules

**Note**

- Fast Ethernet SFPs are supported in these modules:
  - CAT6000-VS-S720-10G/MSFC3
  - ME6524
  - WS-X6148-FE-SFP
- For information about Fast Ethernet SFPs, see the *Cisco 100BASE-X SFP For Fast Ethernet SFP Ports* data sheet:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6578/product_data_sheet0900aecd801f931c.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **GLC-FE-100BX-U** | 100BASE-BX10-U SFP | 12.2(18)SXF2 |
| **GLC-FE-100BX-D** | 100BASE-BX10-D SFP | 12.2(18)SXF2 |
| **GLC-FE-100EX** | 100BASEEX SFP | 12.2(18)SXF |
| **GLC-FE-100ZX** | 100BASEZX SFP | 12.2(18)SXF |
| **GLC-FE-100FX** | 100BASEFX SFP | 12.2(18)SXF |
| **GLC-FE-100LX** | 100BASELX SFP | 12.2(18)SXF |

**Note** GLC-GE-100FX Fast Ethernet SFPs are not supported.

## Gigabit Interface Converters (GBICs)

**Note** The support listed in this section applies to all modules that use GBICs.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WDM-GBIC-REC** | Receive-only wavelength division multiplexing (WDM) GBIC | 12.2(18)SXE |
| **DWDM-GBIC** | Dense wavelength division multiplexing (DWDM) GBIC | 12.2(17a)SX |
| **CWDM-GBIC-1470** | Cisco 1000BASE-CWDM GBIC, 1470 nm (Gray) | 12.2(17a)SX |
| **CWDM-GBIC-1490** | Cisco 1000BASE-CWDM GBIC, 1490 nm (Violet) | |
| **CWDM-GBIC-1510** | Cisco 1000BASE-CWDM GBIC, 1510 nm (Blue) | |
| **CWDM-GBIC-1530** | Cisco 1000BASE-CWDM GBIC, 1530 nm (Green) | |
| **CWDM-GBIC-1550** | Cisco 1000BASE-CWDM GBIC, 1550 nm (Yellow) | |
| **CWDM-GBIC-1570** | Cisco 1000BASE-CWDM GBIC, 1570 nm (Orange) | |
| **CWDM-GBIC-1590** | Cisco 1000BASE-CWDM GBIC, 1590 nm (Red) | |
| **CWDM-GBIC-1610** | Cisco 1000BASE-CWDM GBIC, 1610 nm (Brown) | |
| **WS-G5483** | 1000BASET GBIC | 12.2(14)SX |
| **WS-G5484** | Short wavelength, 1000BASE-SX | 12.2(14)SX |
| **WS-G5486** | Long wavelength/long haul, 1000BASE-LX/LH | 12.2(14)SX |
| **WS-G5487** | Extended distance, 1000BASE-ZX | 12.2(14)SX |

# Shared Port Adapter (SPA) Interface Processors (SIPs)

**Note**

- SIPs are supported only in images that contain "_wan" in the image name.
- See the "FPD Image Packages" section on page 7 for information about additional procedures required to support SIPs with Release 12.2(18)SXE and later releases.

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **7600-SIP-600** | SPA Interface Processor-600<br>**Note**<br>• 7600-SIP-600 has a WS-F6700-DFC3BXL.<br>• Not supported with Supervisor Engine 32.<br>• In Release 12.2(33)SXJ1 and later releases, CDP is disabled by default on 7600-SIP-600 ports (CSCtk12860). | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXI |
| | With Supervisor Engine 720<br>**Note**<br>• Not supported in PFC3A mode.<br>• Not supported in release 12.2(33)SXH and rebuilds. | 12.2(18)SXF<br>12.2(33)SXI |
| **7600-SIP-400** | SPA Interface Processor-400 | |
| | With Supervisor Engine 720-10GE in VSS mode | 12.2(33)SXI4 |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 (not supported in PFC3A mode) | 12.2(18)SXE |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **7600-SIP-200** | SPA Interface Processor-200 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXE |
| | With Supervisor Engine 32 | 12.2(18)SXF |

# Shared Port Adapters (SPAs)

These sections describe SPAs:


- Ethernet SPAs, page 85
- POS SPAs, page 86
- ATM SPAs, page 87
- SFPs for OC3 and OC12 POS and ATM SPAs, page 88
- Serial SPAs, page 88


## Ethernet SPAs

These sections describe Ethernet SPAs:


- 10-Gigabit Ethernet SPAs, page 85
- Gigabit Ethernet SPAs, page 85
- 10/100 Mbps Ethernet SPAs, page 86


### 10-Gigabit Ethernet SPAs

**Note** Release 12.2(33)SXH and rebuilds do not support 7600-SIP-600.

| Product ID (append "=" for spares) | SIP Support | Product Description | Minimum Software Versions |
|---|---|---|---|
| **SPA-1X10GE-L-V2** | 7600-SIP-400 | 1-Port 10 Gigabit Ethernet SPA | 12.2(33)SXI2 |
| **SPA-1XTENGE-XFP** | 7600-SIP-600 | 1-port 10-Gigabit Ethernet SPA | 12.2(33)SXI |
| **XFP Modules Supported in 10-Gigabit Ethernet SPAs** | | | |
| **XFP-10GLR-OC192LR** | 10-Gigabit Ethernet LR (10 km) | | |

### Gigabit Ethernet SPAs

**Note** Release 12.2(33)SXH and rebuilds do not support 7600-SIP-600.

| Product ID (append "=" for spares) | SIP Support | Product Description | Minimum Software Versions |
|---|---|---|---|
| **SPA-10X1GE** | 7600-SIP-600 | 10-port Gigabit Ethernet SPA, SFP Optics | 12.2(33)SXI |
| **SPA-5X1GE-V2** | 7600-SIP-600 | 5-port Gigabit Ethernet SPA, SFP Optics | 12.2(33)SXJ |
| **SPA-5X1GE** | 7600-SIP-600 | 5-port Gigabit Ethernet SPA, SFP Optics | 12.2(33)SXI |

| Product ID (append "=" for spares) | SIP Support | Product Description | Minimum Software Versions |
|---|---|---|---|
| **SPA-2X1GE-V2** | 7600-SIP-400 | 2-port Gigabit Ethernet SPA, SFP Optics, version 2 | 12.2(33)SXI |
| **SPA-2X1GE** | 7600-SIP-400 | 2-port Gigabit Ethernet SPA, SFP Optics | 12.2(18)SXF |
| **SFPs Supported in Gigabit Ethernet SPAs** | | | |
| **SFP-GE-S** | Extended Temperature SX SFP | | 12.2(18)SXF |
| **SFP-GE-L** | Extended Temperature LX/LH SFP | | |
| **SFP-GE-Z** | Extended Temperature ZX SFP | | |
| **SFP-GE-T** | Cisco 1000BASE-T SFP (NEBS 3 ESD) | | 12.2(33)SXH |

### 10/100 Mbps Ethernet SPAs

| Product ID (append "=" for spares) | SIP Support | Product Description | Minimum Software Versions |
|---|---|---|---|
| **SPA-8X1FE-TX-V2** | 7600-SIP-200 | 8-port 10/100 Ethernet SPA TX | 12.2(33)SXH |
| **SPA-4X1FE-TX-V2** | 7600-SIP-200 | 4-port 10/100 Ethernet SPA TX | 12.2(33)SXH |

## POS SPAs

**Note**

- Release 12.2(33)SXH and rebuilds do not support 7600-SIP-600.
- With Release 12.2(33)SXI and later releases where CSCso97991 is not resolved, you must configure an appropriate burst size when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.

| Product ID (append "=" for spares) | SIP Support | Product Description | Minimum Software Versions |
|---|---|---|---|
| **SPA-OC192POS-VSR** | 7600-SIP-600 | 1-port OC-192c/STM-64 POS/RPR SPA, VSR-1 | 12.2(33)SXI |
| **SPA-OC192POS-LR** | 7600-SIP-600 | 1-port OC-192c/STM-64 POS/RPR SPA, SM-LR | 12.2(33)SXI |
| **SPA-OC192POS-XFP** | 7600-SIP-600 | 1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics | 12.2(33)SXI |
| | | **XFP Modules Supported in SPA-OC192POS-XFP** | |
| | | XFP-10GLR-OC192SR Single-Mode (SM) Short Reach (SR) | |
| | | XFP-10GER-OC192IR Single-Mode (SM) Intermediate Reach (IR-2) | |
| **SPA-OC192POS-VSR** | 7600-SIP-600 | 1-port OC-192c/STM-64 POS/RPR SPA, VSR-1 | 12.2(33)SXI |
| **SPA-2XOC48POS/RPR** | 7600-SIP-400 | 2-Port OC-48 POS/RPR SPA<br>**Note** Requires SFPs. | 12.2(33)SXI |

| Product ID (append "=" for spares) | SIP Support | Product Description | Minimum Software Versions |
|---|---|---|---|
| SPA-1XOC48POS/RPR | 7600-SIP-400 | 1-Port OC-48 POS/RPR SPA<br>**Note** Requires SFPs. | 12.2(18)SXF10 |
| SPA-2XOC3-POS | 7600-SIP-200<br>7600-SIP-400 | 2-port OC-3c/STM-1c POS SPA<br>**Note** Requires SFPs. | 12.2(18)SXE |
| SPA-4XOC3-POS | 7600-SIP-200<br>7600-SIP-400 | 4-port OC-3c/STM-1c POS SPA<br>**Note** Requires SFPs. | 12.2(18)SXE |
| SPA-1XOC12-POS | 7600-SIP-400 | 1-port OC-12c/STM-4c POS SPA<br>**Note** Requires an SFP. | 12.2(18)SXE |

## ATM SPAs

**Note**

- Release 12.2(33)SXH and rebuilds do not support ATM SPAs.
- With Release 12.2(33)SXI and later releases where CSCso97991 is not resolved, you must configure an appropriate burst size when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.

| Product ID (append "=" for spares) | SIP Support | Product Description | Minimum Software Versions |
|---|---|---|---|
| SPA-1XOC12-ATM | 7600-SIP-400 | 1-Port OC-12c/STM-4c ATM SPA<br>**Note** Requires an SFP. | 12.2(18)SXE |
| SPA-2XOC3-ATM | 7600-SIP-200<br>7600-SIP-400 | 2-port OC-3c/STM-1c ATM SPA<br>**Note** Requires SFPs. | 12.2(18)SXE |
| SPA-4XOC3-ATM | 7600-SIP-200<br>7600-SIP-400 | 4-port OC-3c/STM-1c ATM SPA<br>**Note** Requires SFPs. | 12.2(18)SXE |
| SPA-1XOC48-ATM | 7600-SIP-400 | 1 port OC-48c/STM-16 ATM SPA | 12.2(18)SXF |

## SFPs for OC3 and OC12 POS and ATM SPAs

| Product ID (append "=" for spares) | Product Description |
|---|---|
| **SFP-OC3-MM** | OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector |
| **SFP-OC3-SR** | OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector |
| **SFP-OC3-IR1** | OC-3/STM-1 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength, LC connector |
| **SFP-OC3-LR1** | OC-3/STM-1 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector |
| **SFP-OC3-LR2** | OC-3/STM-1 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector |
| **SFP-OC12-MM** | OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector |
| **SFP-OC12-SR** | OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector |
| **SFP-OC12-IR1** | OC-12/STM-4 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength |
| **SFP-OC12-LR1** | OC-12/STM-4 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector |
| **SFP-OC12-LR2** | OC-12/STM-4 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector |

## Serial SPAs

**Note** With Release 12.2(33)SXI and later releases where CSCso97991 is not resolved, you must configure an appropriate burst size when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.

| Product ID (append "=" for spares) | Product Description | SIP Support | Minimum Software Versions |
|---|---|---|---|
| **SPA-1xCHSTM1/OC3** | 1-port Channelized STM1/OC3 to DS0 SPA | 7600-SIP-200 | 12.2(33)SXH |
| **SPA-2XCT3/DS0** | 2-port Channelized T3 to DS0 SPA | | |
| | | 7600-SIP-400 | 12.2(33)SXI |
| | | 7600-SIP-200 | 12.2(18)SXE |
| **SPA-4XCT3/DS0** | 4-port Channelized T3 to DS0 SPA | | |
| | | 7600-SIP-400 | 12.2(33)SXI |
| | | 7600-SIP-200 | 12.2(18)SXE |

| Product ID (append "=" for spares) | Product Description | SIP Support | Minimum Software Versions |
|---|---|---|---|
| **SPA-8XCHT1/E1** | 8-Port Channelized T1/E1 SPA | | |
| | | 7600-SIP-400 | 12.2(33)SXI |
| | | 7600-SIP-200 | 12.2(18)SXE |
| **SPA-2XT3/E3** | 2-port Clear Channel T3/E3 SPA | | |
| | | 7600-SIP-400 | 12.2(33)SXI |
| | | 7600-SIP-200 | 12.2(18)SXE |
| **SPA-4XT3/E3** | 4-port Clear Channel T3/E3 SPA | | |
| | | 7600-SIP-400 | 12.2(33)SXI |
| | | 7600-SIP-200 | 12.2(18)SXE |

# Services SPA Carrier (SSC) and Services SPAs

**Note** If you are upgrading from a Release 12.2(18)SXF or rebuild image to a Release 12.2(33)SXH or later image, be aware of CSCsv30090, "SPA-IPsec-2G VRF: vlan 1 mistakenly trunked on upgrade from SXF to SXH."

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-SSC-600**<br>**WS-IPSEC-3** | Services SPA Carrier (SSC) and IPsec SPA | |
| | With Supervisor Engine 720-10GE in VSS mode | 12.2(33)SXJ1 |
| | With Supervisor Engine 720-10GE | 12.2(33)SXI |
| | With Supervisor Engine 720 | |
| | With Supervisor Engine 32 | |
| **7600-SSC-400**<br>**SPA-IPSEC-2G** | Services SPA Carrier (SSC) and IPsec SPA<br>**Note**<br>• 7600-SSC-400 does not maintain state when an NSF with SSO redundancy mode switchover occurs.<br>• See the "FPD Image Packages" section on page 7 for information about additional procedures required to support SPA-IPSEC-2G with Release 12.2(18)SXE and later releases.<br>• SPA-IPSEC-2G does not support TACACS+ authentication for IPsec. | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXE2 |
| | With Supervisor Engine 32 | 12.2(18)SXF2 |

# Enhanced FlexWAN Module

**Note**

- Supported only in images that contain "_wan" in the image name.
- With Release 12.2(33)SXI and later releases where CSCso97991 is not resolved, you must configure an appropriate burst size when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.

| Product ID (append "=" for spares) | Product Description | Minimum Software Version |
|---|---|---|
| **WS-X6582-2PA** | Enhanced FlexWAN Module; CEF256 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(17b)SXA |
| | With Supervisor Engine 32 | 12.2(18)SXF |

# Enhanced FlexWAN Module Port Adapters

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **PA-2FE** | 2-port Fast Ethernet Port Adapter | 12.2(18)SXE |
| **PA-1FE** | 1-port Fast Ethernet Port Adapter | 12.2(18)SXE |
| **PA-POS-1OC3** | 1-port Packet over SONET OC3c/STM1 Port Adapter | 12.2(18)SXE |
| **PA-POS-2OC3** | 2-port POS OC3c/STM1<br>• SFPs for PA-POS-2OC3:<br>– SFP-OC3-MM, short range, multimode fiber<br>– SFP-OC3-IR1, intermediate range, single-mode fiber<br>– SFP-OC3-LR1, long range, single-mode fiber | 12.2(17b)SXA |
| **PA-POS-OC3MM**<br>**PA-POS-OC3SMI**<br>**PA-POS-OC3SML** | Packet over SONET (OC-3) | 12.2(14)SX |
| **PA-A6-OC3MM** | 1-port ATM OC-3c/STM-1 multimode port adapter, enhanced | 12.2(14)SX |
| **PA-A6-OC3SMI** | 1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced | 12.2(14)SX |
| **PA-A6-OC3SML** | 1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced | 12.2(14)SX |
| **PA-A6-T3** | 1-port ATM DS3 port adapter, enhanced | 12.2(14)SX |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **PA-A6-E3** | 1-port ATM E3 port adapter, enhanced | 12.2(14)SX |
| **PA-A3-OC3MM**<br>**PA-A3-OC3SMI**<br>**PA-A3-T3**<br>**PA-A3-OC3SML**<br>**PA-A3-E3**<br>**PA-A3-8T1IMA**<br>**PA-A3-8E1IMA** | ATM with traffic shaping<br>**Note** These port adapters do not support LANE when installed in the FlexWAN module. | 12.2(14)SX |
| **PA-T3**<br>**PA-T3+**<br>**PA-2T3**<br>**PA-2T3+**<br>**PA-E3**<br>**PA-2E3**<br>**PA-MC-T3**<br>**PA-MC-E3**<br>**PA-MC-2T3+** | T3/E3 (clear-channel and channelized) | 12.2(14)SX |
| **PA-4T+**<br>**PA-8T-V35**<br>**PA-8T-X21**<br>**PA-8T-232**<br>**PA-MC-2E1/120**<br>**PA-MC-8T1**<br>**PA-MC-8E1/120**<br>**PA-MC-2T1**<br>**PA-MC-4T1** | T1/E1 | 12.2(14)SX |
| **PA-4E1G/75**<br>**PA-4E1G/120** | T1/E1 | 12.2(17)SX |
| **PA-MC-8TE1+** | Multichannel T1/E1 8PRI<br>**Note** This port adapter does not support ISDN PRI when installed in the FlexWAN module. | 12.2(14)SX |
| **PA-H**<br>**PA-2H** | HSSI | 12.2(14)SX |
| **PA-MC-STM-1** | Multichannel STM-1 | 12.2(14)SX |

# Service Modules


- Application Control Engine (ACE) Module, page 92
- Anomaly Guard Module(AGM), page 93
- Traffic Anomaly Detector Module (ADM), page 93
- ASA Services Module, page 93
- Communication Media Module (CMM), page 94
- Content Switching Module (CSM), page 95
- Content Switching Module with SSL (CSM-S), page 95
- Firewall Services Module (FWSM), page 96

- Intrusion Detection System Modules (IDSMs), page 96
- Network Analysis Modules (NAMs), page 97
- Secure Sockets Layer (SSL) Services Module, page 98
- Wireless Services Modules, page 98


**Note**

- For service modules that run their own software, see the service module software release notes for information about the minimum required service module software version.
- With SPAN configured to include a port-channel interface to support a service module, be aware of CSCth03423 and CSCsx46323.
- EtherChannel configuration can impact some service modules. In particular, distributed EtherChannels (DECs) can interfere with service module traffic. See this field notice for more information:

  http://www.cisco.com/en/US/ts/fn/610/fn61935.html

## Application Control Engine (ACE) Module

**Note**

- ACE30-MOD-K9, ACE10-6500-K9, and ACE20-MOD-K9 run their own software—See these publications:

  http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

  See the module software release notes for information about the minimum required service module software version.

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **ACE30-MOD-K9** | Application Control Engine (ACE) module | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXI4 |
| | With Supervisor Engine 720 | |
| **ACE10-6500-K9**<br>**ACE20-MOD-K9** | Application Control Engine (ACE) module<br>**Note** With releases earlier than Release 12.2(33)SXI, not supported in virtual switch mode. | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF4 |

## Anomaly Guard Module(AGM)

**Note**

- WS-SVC-AGM-1-K9 runs its own software—See these publications:

  http://www.cisco.com/en/US/products/ps6236/tsd_products_support_model_home.html
- See the WS-SVC-AGM-1-K9 software release notes for information about the minimum required WS-SVC-AGM-1-K9 software version.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-SVC-AGM-1-K9** | Anomaly Guard Module (AGM) | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH1 |
| | With Supervisor Engine 720 | 12.2(18)SXD3 |

## Traffic Anomaly Detector Module (ADM)

**Note**

- WS-SVC-ADM-1-K9 runs its own software—See these publications:

  http://www.cisco.com/en/US/products/ps6236/tsd_products_support_model_home.html
- See the WS-SVC-ADM-1-K9 software release notes for information about the minimum required WS-SVC-ADM-1-K9 software version.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-SVC-ADM-1-K9** | Traffic Anomaly Detector Module (ADM) | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH1 |
| | With Supervisor Engine 720 | 12.2(18)SXD3 |

## ASA Services Module

**Note**

- Supported only with 6500 E-series chassis: WS-C6513-E, WS-C6509-V-E, WS-C6509-E, WS-C6506-E, WS-C6504-E, and WS-C6503-E.
- Not supported in PFC3A mode.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-SVC-ASA-SM1-K9** | ASA Services Module | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXJ1 |
| | With Supervisor Engine 720 | |

## Communication Media Module (CMM)

**Note**

- WS-SVC-CMM runs its own software—See these publications:

  http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/cmm/release/notes/OL_4847.html

- See the WS-SVC-CMM software release notes for information about the minimum required WS-SVC-CMM software version.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-SVC-CMM** | Communication Media Module | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **Communication Media Module Port Adapters for WS-SVC-CMM** | | |
| **WS-SVC-CMM-6E1** | 6-Port E1 Interface Port Adapter | |
| **WS-SVC-CMM-6T1** | 6-Port T1 Interface Port Adapter | |
| **WS-SVC-CMM-ACT** | Adhoc Conferencing and Transcoding Port Adapter | |
| **WS-SVC-CMM-24FXS** | 24-Port FXS Interface Port Adapter | |

## Content Switching Module (CSM)

**Note**

- WS-X6066-SLB-APC runs its own software—See these publications:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/tsd_products_support_model_home.html

- See the WS-X6066-SLB-APC software release notes for information about the minimum required WS-X6066-SLB-APC software version.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6066-SLB-APC** | Content Switching Module (CSM) | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXI2<br>(Not supported in Release 12.2(33)SXJ and rebuilds) |
| | With Supervisor Engine 720 | |

## Content Switching Module with SSL (CSM-S)

**Note**

- WS-X6066-SLB-S-K9 runs its own software—See these publications:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/tsd_products_support_model_home.html

- See the WS-X6066-SLB-S-K9 software release notes for information about the minimum required WS-X6066-SLB-S-K9 software version.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-X6066-SLB-S-K9** | Content Switching Module with SSL (CSM-S) | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXI2<br>(Not supported in Release 12.2(33)SXJ and rebuilds) |
| | With Supervisor Engine 720 | |

## Firewall Services Module (FWSM)

**Note**

- With Firewall Services Module Software Release 2.3(1) and later releases, WS-SVC-FWM-1-K9 maintains state when an NSF with SSO redundancy mode switchover occurs.
- The FWSM runs its own software—See these publications:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-SVC-FWM-1-K9** | Firewall Services Module; CEF256 | |
| | With Supervisor Engine 720-10GE in VSS mode | 12.2(33)SXI |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX1 |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## Intrusion Detection System Modules (IDSMs)

**Note**

- The IDSM runs its own software—See these publications:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/tsd_products_support_model_home.html

  See the IDSM software release notes for information about the minimum required IDSM software version.

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-SVC-IDSM2-K9** | Intrusion Detection System Module 2; CEF256 | |
| | With Supervisor Engine 720-10GE in VSS mode | 12.2(33)SXI |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX1 |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## Network Analysis Modules (NAMs)

**Note**

- Network Analysis Modules run their own software—See this publication for more information: http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_notes_list.html
- See the NAM software release notes for information about the minimum required NAM software version.

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-SVC-NAM3-6G-K9** | Network Analysis Module 3 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXJ1 |
| | With Supervisor Engine 720 | |
| | • Supported only with 6500 E-series chassis: WS-C6513-E, WS-C6509-V-E, WS-C6509-E, WS-C6506-E, WS-C6504-E, and WS-C6503-E.<br>• Not supported in PFC3A mode. | |
| **WS-SVC-NAM-2**<br>**WS-SVC-NAM-1** | Network Analysis Module 2<br>Network Analysis Module 1 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX1 |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## Secure Sockets Layer (SSL) Services Module

**Note**

- Supported in virtual switch mode.
- WS-SVC-SSL-1 does not maintain state when an NSF with SSO redundancy mode switchover occurs.
- WS-SVC-SSL-1 runs its own software—See the publications listed here for more information:

  http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html
- See the WS-SVC-SSL-1 software release notes for information about the minimum required WS-SVC-SSL-1 software version.

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-SVC-SSL-1** | Secure Sockets Layer (SSL) Services Module | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXI4 |
| | With Supervisor Engine 720 | • 12.2(33)SXI4a or later recommended<br>• Not supported in Release 12.2(33)SXJ and rebuilds |
| | With Supervisor Engine 32 | |

## Wireless Services Modules


- Wireless Services Module 2 (WiSM2), page 99
- Wireless Services Module (WiSM), page 99

### Wireless Services Module 2 (WiSM2)

**Note**

- Supervisor Engine 32 does not support WS-SVC-WISM2-K9.
- In a 13-slot chassis, WS-SVC-WISM2-K9 is supported only in slots 9 through 13 and does not power up in other slots.
- WS-SVC-WISM2-K9 runs its own software—See these publications:

  http://www.cisco.com/en/US/products/ps10315/prod_release_notes_list.html
- See the WS-SVC-WISM2-K9 software release notes for information about the minimum required WS-SVC-WISM-1-K9 software version.

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-SVC-WISM2-K9** | Wireless Services Module 2 (WiSM2) | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXJ |
| | With Supervisor Engine 720 | |

### Wireless Services Module (WiSM)

**Note**

- With releases earlier than Release 12.2(33)SXI, not supported in virtual switch mode.
- In a 13-slot chassis, WS-SVC-WISM-1-K9 is supported only in slots 9 through 13 and does not power up in other slots.
- WS-SVC-WISM-1-K9 runs its own software—See these publications:

  http://www.cisco.com/en/US/products/ps6526/tsd_products_support_model_home.html
- See the WS-SVC-WISM-1-K9 software release notes for information about the minimum required WS-SVC-WISM-1-K9 software version.

| **Product ID** (append "=" for spares) | **Product Description** | **Minimum Software Versions** |
|---|---|---|
| **WS-SVC-WISM-1-K9** | Wireless Services Module (WiSM) | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF2 |

# Fan Trays

**Note** Enter the **show environment status | include fan** command or the **show environment cooling** command to display information about the installed fan trays.

| Product ID (append "=" for spares) | Product Description | Minimum Software Version |
|---|---|---|
| **FAN-MOD-3HS** | High-capacity fan tray for WS-C6503 and CISCO7603 chassis | 12.2(14)SX |
| **FAN-MOD-6HS** | High-capacity fan tray for CISCO7606 chassis | 12.2(14)SX |
| **WS-C6K-6SLOT-FAN2** | High-capacity fan tray for WS-C6506 chassis | 12.2(14)SX |
| **FAN-MOD-09** | High-capacity fan tray for WS-C6509-NEB-A and CISCO7609 chassis | 12.2(14)SX |
| **WS-C6K-9SLOT-FAN2** | High-capacity fan tray for WS-C6509 chassis | 12.2(14)SX |
| **WS-C6K-13SLT-FAN2** | High-capacity fan tray for WS-C6513 and CISCO7613 chassis | 12.2(14)SX |

# Power Supplies


- CISCO7606 Power Supplies, page 100
- WS-C6504-E and CISCO7604 Power Supplies, page 101
- WS-C6503, WS-C6503-E, and CISCO7603 Power Supplies, page 101
- All Other Power Supplies, page 101


## CISCO7606 Power Supplies

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **PWR-2700-AC** | 2700 W AC power supply | 12.2(18)SXE |
| **PWR-2700-DC** | 2700 W DC power supply | 12.2(18)SXE |

## WS-C6504-E and CISCO7604 Power Supplies

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **PWR-2700-AC/4** | 2700 W AC power supply | 12.2(18)SXE |
| **PWR-2700-DC/4** | 2700 W DC power supply | 12.2(18)SXE |

## WS-C6503, WS-C6503-E, and CISCO7603 Power Supplies

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **PWR-1400-AC** | 1,400 W AC power supply | 12.2(17a)SX |
| **PWR-950-AC** | 950 W AC power supply | 12.2(14)SX |
| **PWR-950-DC** | 950 W DC power supply | 12.2(14)SX |

## All Other Power Supplies

**Note** The power supplies in this section are not supported in these chassis:

- Catalyst 6503
- Catalyst 6503-E
- CISCO7603
- Catalyst 6504-E
- CISCO7604

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-CAC-8700W-E** | 8,700 W AC power supply | 12.2(18)SXF8 |
| | **Note**<br>• Limited to 4,500 W inthe WS-C6509-NEB-A chassis.<br>• Limited to 4,000 W in these chassis:<br>– WS-C6509<br>– WS-C6506<br>– WS-C6509-NEB<br>• WS-CAC-8700W-E supports a remote power cycling feature.<br>• See this publication for more information:<br>http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html | |
| **PWR-6000-DC** | 6,000 W DC power supply | 12.2(18)SXF13<br>12.2(33)SXH2 |
| | **Note**<br>• Limited to 4,500 W in the WS-C6509-NEB-A chassis.<br>• Limited to 4,000 W in these chassis:<br>– WS-C6509<br>– WS-C6506<br>– WS-C6509-NEB | |
| **WS-CAC-6000W** | 6,000 W AC power supply | 12.2(18)SXD |
| | **Note**<br>• Limited to 4,500 W inthe WS-C6509-NEB-A chassis.<br>• Limited to 4,000 W in these chassis:<br>– WS-C6509<br>– WS-C6506<br>– WS-C6509-NEB | |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **PWR-4000-DC** | 4,000 W DC power supply | 12.2(14)SX |
| **WS-CAC-4000W** | 4,000 W AC power supply | 12.2(14)SX |
| **+WS-CAC-3000W** | 3,000 W AC power supply | 12.2(17a)SX |
| | **Note**<br>• Required with Supervisor Engine 720 or Supervisor Engine 720-10GE in WS-C6509-NEB or OSR7609.<br>• Included in the WS-6509-NEB-UPGRD= upgrade kit. | |
| **WS-CAC-3000W** | 3,000 W AC power supply | 12.2(14)SX |
| **WS-CAC-2500W** | 2,500 W AC power supply | 12.2(14)SX |
| **WS-CDC-2500W** | 2,500 W DC power supply | 12.2(14)SX |

# Chassis


- 13-Slot Chassis, page 104
- 9-Slot Chassis, page 105
- 6-Slot Chassis, page 108
- 4-Slot Chassis, page 109
- 3-Slot Chassis, page 109

## 13-Slot Chassis

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-C6513-E** | Catalyst 6513-E chassis:<br>• 13 slots<br>• 64 chassis MAC addresses<br>• These modules are supported only in slots 9 through 13 and do not power up in other slots:<br>– WS-X6700 series switching modules except WS-X6724-SFP<br>– WS-X6816-GBIC switching modules<br>– WS-SVC-WISM-1-K9 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXI1<br>12.2(33)SXH2 |
| | With Supervisor Engine 720 | 12.2(33)SXI1<br>12.2(33)SXH2<br>12.2(18)SXF14 |
| | With Supervisor Engine 32 | 12.2(33)SXI1<br>12.2(33)SXH2<br>12.2(18)SXF14 |
| **WS-C6513** | Catalyst 6513 chassis:<br>• 13 slots<br>• 64 chassis MAC addresses<br>• Use with Supervisor Engine 720-10GE or Supervisor Engine 720 requires WS-C6K-13SLT-FAN2<br>• These modules are supported only in slots 9 through 13 and do not power up in other slots:<br>– WS-X6700 series switching modules except WS-X6724-SFP<br>– WS-X6816-GBIC switching modules<br>– WS-SVC-WISM-1-K9 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| CISCO7613 | Cisco 7613 chassis:<br>• 13 slots<br>• 64 chassis MAC addresses<br>• Use with Supervisor Engine 720-10GE or Supervisor Engine 720 requires WS-C6K-13SLT-FAN2<br>• These modules are supported only in slots 9 through 13 and do not power up in other slots:<br>– WS-X6700 series switching modules<br>– WS-X6816-GBIC switching modules<br>– WS-SVC-WISM-1-K9 | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode). | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## 9-Slot Chassis

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| WS-C6509-V-E | Catalyst 6509-V-E chassis:<br>• 9 vertical slots<br>• 64 chassis MAC addresses<br>• Required power supply:<br>– 2,500 W DC or higher<br>– 3,000 W AC or higher | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXF10 |
| | With Supervisor Engine 32 | 12.2(18)SXF10 |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-C6509-E** | Catalyst 6509-E chassis:<br>• 9 horizontal slots<br>• Chassis MAC addresses:<br>– Before April 2009—1024 chassis MAC addresses<br>– Starting in April 2009—64 chassis MAC addresses<br>**Note** Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.**<br>• Requires 2,500 W or higher power supply<br>• With releases earlier than Release 12.2(18)SXD, WS-CAC-6000W is limited to 4,000 W in WS-C6509-E | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **WS-C6509** | Catalyst 6509 chassis:<br>• 9 horizontal slots<br>• 1024 chassis MAC addresses<br>• Use with Supervisor Engine 720-10GE, Supervisor Engine 720, or Supervisor Engine 32 requires WS-C6K-9SLOT-FAN2<br>• WS-CAC-6000W is limited to 4,000 W in WS-C6509 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **WS-C6509-NEB-A** | Catalyst 6509-NEB chassis<br>• 9 vertical slots<br>• 64 chassis MAC addresses<br>• Supports two FAN-MOD-09 modules.<br>• Two FAN-MOD-09 modules required with WS-X6716-10G or WS-X6708-10GE. | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-C6509-NEB** | Catalyst 6509-NEB chassis:<br>• 9 vertical slots<br>• 1024 chassis MAC addresses<br>• Requires the WS-6509-NEB-UPGRD= upgrade kit—refer to this publication:<br>http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16162.html<br>• Does not support WS-X6716-10T-3C or WS-X6716-10T-3CXL. | |
| | With Supervisor Engine 720 | 12.2(17a)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **CISCO7609** | Cisco 7609 chassis<br>• 9 vertical slots<br>• 64 chassis MAC addresses | |
| | With Supervisor Engine 720-10GE (Not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **OSR-7609** | Cisco 7609 chassis:<br>• 9 vertical slots<br>• 1024 chassis MAC addresses<br>• Requires the WS-6509-NEB-UPGRD= upgrade kit—refer to this publication:<br>http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16162.html | |
| | With Supervisor Engine 720 | 12.2(17a)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## 6-Slot Chassis

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| **WS-C6506-E** | Catalyst 6506 chassis:<br>• 6 slots<br>• Chassis MAC addresses:<br>– Before April 2009—1024 chassis MAC addresses<br>– Starting in April 2009—64 chassis MAC addresses<br>**Note** Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.**<br>• Requires 2,500 W or higher power supply | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **WS-C6506** | Catalyst 6506 chassis:<br>• 6 slots<br>• 1024 chassis MAC addresses<br>• Requires WS-C6K-6SLOT-FAN2<br>• WS-CAC-6000W limited to 4,000 W in WS-C6506 | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| **CISCO7606** | Cisco 7606 chassis:<br>• 6 slots<br>• 64 chassis MAC addresses<br>• Requires FAN-MOD-6HS | |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## 4-Slot Chassis

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| WS-C6504-E | Catalyst 6504-E chassis:<br>• 4 slots<br>• 64 chassis MAC addresses | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(18)SXE |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| CISCO7604 | Cisco 7604 chassis:<br>• 4 slots<br>• 64 chassis MAC addresses | |
| | With Supervisor Engine 720-10GE (not supported in VSS mode) | 12.2(33)SXH |
| | With Supervisor Engine 720: | 12.2(18)SXE |
| | With Supervisor Engine 32 | 12.2(18)SXF |

## 3-Slot Chassis

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| WS-C6503-E | • 3 slots<br>• 64 chassis MAC addresses | |
| | With Supervisor Engine 720-10GE | 12.2(33)SXH |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |
| WS-C6503 | Catalyst 6503 chassis:<br>• 3 slots<br>• 64 chassis MAC addresses<br>• Requires FAN-MOD-3HS<br>• Does not support:<br>– WS-X6700 series switching modules<br>– WS-X6816-GBIC switching modules<br>– Supervisor Engine 720-10GE | |
| | With Supervisor Engine 720 | 12.2(14)SX |
| | With Supervisor Engine 32 | 12.2(18)SXF |

| Product ID (append "=" for spares) | Product Description | Minimum Software Versions |
|---|---|---|
| CISCO7603 | Cisco 7603 chassis:<br>• 3 slots<br>• 64 chassis MAC addresses<br>• Use with Supervisor Engine 720-10GE or Supervisor Engine 720 requires FAN-MOD-3HS<br>• Does not support:<br>– WS-X6700 series switching modules<br>– WS-X6816-GBIC switching modules<br>– Supervisor Engine 720-10GE<br>– Supervisor Engine 32 | |
| | With Supervisor Engine 720 | 12.2(14)SX |

# Cisco ME 6500 Series Ethernet Switches (ME6524)


- Cisco ME 6500 Series Ethernet Switches Restrictions, page 110
- Cisco ME 6500 Series Ethernet Switches Features, page 111


## Cisco ME 6500 Series Ethernet Switches Restrictions

Cisco ME 6500 Series Ethernet switches cannot support these software features and commands:

- Cisco ME 6500 Series Ethernet switches are not supported in Release 12.2(33)SXJ and later releases. Support continues in Release 12.2(33)SXI and rebuilds.
- Egress multicast replication
- Multicast replication mode detection
- Fabric configuration commands
- RPR and SSO redundancy
- VLAN translation

## Cisco ME 6500 Series Ethernet Switches Features

| Product ID (append "=" for spares) | Product Description | Minimum Software Version |
|---|---|---|
| **ME-C6524GS-8S**<br>**ME-C6524GT-8S** | Cisco ME 6500 Series Ethernet switches:<br>• Switch processor (SP):<br>– For Cisco IOS images, 256-MB DRAM (some images require more DRAM)<br>– For Cisco IOS modularity images, with releases earlier than Release 12.2(33)SXH3, 256-MB DRAM (some images require more DRAM)<br>– For Cisco IOS modularity images, with Release 12.2(33)SXH3 and later releases, 512-MB DRAM required (some images require more DRAM)<br>– 128-MB bootflash (**sup-bootflash:**; from ROMMON, it is **bootflash:**)<br>• Route processor (RP)—Multilayer Switch Feature Card 2A (MSFC2A):<br>– 512-MB DRAM (some images require more DRAM)<br>– 64-MB bootflash (**bootflash:**)<br>• Policy Feature Card 3C (PFC3C)<br>– See the "Policy Feature Cards" section on page 24<br>– ME 6500 switches always operate in PFC3C mode. Enter the **show platform hardware pfc mode** command to display the PFC3 mode.<br>• Fan tray: FAN-C6524<br>• Power supplies (can be used together):<br>– PWR-400W-DC<br>– PWR-400W-AC<br>• 64 chassis MAC addresses<br>• One external CompactFlash Type II slot (**disk0:**; supports CompactFlash Type II Flash PC cards sold by Cisco Systems, Inc., for use in Cisco ME 6500 Series Ethernet switches)<br>• Eight SFP ports:<br>– Requires Small Form-Factor Pluggable (SFP) Modules<br>– 1 port group: ports 25–32<br>– QoS port architecture (Rx/Tx): **2q8t/1p3q8t**<br>• ME-C6524GS-8S:<br>– 24 SFP ports (requires Small Form-Factor Pluggable (SFP) Modules)<br>– 4 port groups: ports 1–6, 7–12, 13–18, 19–24<br>– QoS port architecture (Rx/Tx): **1q2t/1p3q8t**<br>• ME-C6524GT-8S:<br>– 24 10/100/1000 Mbps RJ-45 Ethernet ports<br>– 4 port groups: ports 1–6, 7–12, 13–18, 19–24<br>– QoS port architecture (Rx/Tx): **1q2t/1p3q8t** | 12.2(33)SXH |

**Note** See this publication for Cisco ME 6500 Series Ethernet switch hardware information:

http://www.cisco.com/en/US/products/ps6845/tsd_products_support_eol_series_home.html

# Unsupported Hardware

**Note**

- See the "Supervisor Engine 32 (CAT6000-SUP32/MSFC2A)" section on page 22 for information about hardware that is not supported with the Supervisor Engine 32.
- See the *Release Notes for Cisco IOS Release 12.2SXF and Rebuilds* publication for information about support in earlier releases:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html

Release 12.2(33)SXH and later releases do not support the following hardware:

- Supervisor Engine 1 (WS-X6K-S1A-MSFC2, WS-X6K-SUP1A-MSFC)
- Supervisor Engine 2 (WS-X6K-S2U-MSFC2, WS-X6K-S2-MSFC2 )
- WS-F6K-DFC distributed forwarding card (DFC)
- Optical Services Modules (OSMs)
- These service modules:
  - WS-X6381-IDS Intrusion Detection System (IDS) Module (WS-SVC-IDSM2-K9 is supported)
  - WS-X6380-NAM Network Analysis Module (NAM; WS-SVC-NAM-2 and WS-SVC-NAM-1 are supported)
  - WS-SVC-AON-1-K9 Application-Oriented Networking (AON) Module
  - WS-SVC-CSG-1 Content Services Gateway (CSG) Module
  - WS-SVC-IPSEC-1 IPsec VPN Acceleration Services Module
  - WS-SVC-MWAM-1 Multi-Processor WAN Application Module
  - WS-SVC-PSD-1 Persistent Storage Device Module
  - WS-SVC-WEBVPN-K9 WebVPN Services Module
  - WS-SVC-WLAN-1-K9 Wireless LAN service module
- Release 12.2(33)SXI and rebuilds support the 7600-SIP-600. Release 12.2(33)SXH and rebuilds do not support the 7600-SIP-600 and these SPAs:
  - SPA-10X1GE 10-port Gigabit Ethernet SPA, SFP Optics
  - SPA-5X1GE 5-port Gigabit Ethernet SPA, SFP Optics
  - SPA-1XTENGE-XFP 1-port 10-Gigabit Ethernet SPA, LANPHY XFP Optics
  - SPA-OC192POS-VSR 1-port OC-192c/STM-64 POS/RPR SPA, VSR-1
  - SPA-OC192POS-LR 1-port OC-192c/STM-64 POS/RPR SPA, SM-LR
  - SPA-OC192POS-XFP 1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics
  - SPA-OC192POS-VSR 1-port OC-192c/STM-64 POS/RPR SPA, VSR-1
- WS-X6182-2PA FlexWAN Module
- These Ethernet Switching Modules:
  - WS-X6024-10FL-MT 24-port 10BASE-FL MT-RJ
  - WS-X6248A-TEL 48-port 10/100TX RJ-21

  - WS-X6248-RJ-45 48-port 10/100TX RJ-45
  - WS-X6248-TEL 48-port 10/100TX RJ-21
  - WS-X6324-100FX-SM 24-port 100FX Ethernet
  - WS-X6224-100FX-MT 24-port 100FX Ethernet Multimode MT-RJ
  - WS-X6316-GE-TX 16-port Gigabit Ethernet RJ-45
  - WS-X6416-GE-MT 16-Port Gigabit Ethernet MT-RJ
- WS-CAC-1000W power supply
- WS-CAC-1300W power supply
- WS-CDC-1300W power supply
- These fan trays:
  - FAN-MOD-3
  - FAN-MOD-6
  - WS-C6K-6SLOT-FAN
  - WS-C6509-NEB-FAN
  - WS-C6K-9SLOT-FAN
  - WS-C6K-13SLT-FAN
- With a Supervisor Engine 720, WS-X6516-GBIC hardware revisions 5.0 through 5.4 with a DFC3 installed.

  Supervisor Engine 720 supports a DFC3 on these WS-X6516-GBIC hardware revisions:

  - Lower than 5.0
  - 5.5 and higher

  With a Supervisor Engine 720 and a DFC3 installed, WS-X6516-GBIC hardware revisions 5.0 through 5.3 do not power up. Without a DFC3, WS-X6516-GBIC hardware revisions 5.0 through 5.4 operate in bus mode.

  See external field notice 24494 for more information:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html
- WS-X6624-FXS, WS-X6608-T1, and WS-X6608-E1 voice modules
- WS-X6101-OC12-MMF and WS-X6101-OC12-SMF ATM LANE modules
- WS-X6302-MSM Multilayer Switch Module
- Catalyst 6000 series chassis

Unsupported modules remain powered down if detected and do not affect system behavior.

# Feature Sets

These sections describe the feature sets in Release 12.2SX:


- Feature Set Guidelines and Restrictions, page 115
- Feature Set Descriptions, page 115


## Feature Set Guidelines and Restrictions

These are the feature set guidelines and restrictions:

- The FlexWAN and Enhanced FlexWAN modules and SIPs and SPAs are supported only in images that contain "_wan" in the image name.
- This product bulletin explains the feature sets used in Release 12.2(18)SXE and later releases:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps5460/prod_bulletin0900aecd80281b17_ps708_Products_Bulletin.html
- The releases includes strong encryption images. Strong encryption images are subject to U.S. and local country export, import, and use laws. The country and class of end users eligible to receive and use Cisco encryption solutions are limited. See this publication for more information:

  http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html
- Some TFTP server implementations cannot transfer 16 MB or larger files. To transfer 16 MB or larger files, you might need to use FTP or rcp. See this online publication for procedures:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf008.html

## Feature Set Descriptions

This section lists all of the features that are unique to each feature set and some of the features that are common to all feature sets.

| Feature Name | IP Base | IP Services | Advanced IP Services | Enterprise Services | Advanced Enterprise Services |
|---|---|---|---|---|---|
| TCP Intercept | | | | | X |
| IPsec Network Security<br>**Note**<br>• The SPA-IPSEC-2G supports IPsec Network Security in hardware.<br>• Without a SPA-IPSEC-2G, the IPsec Network Security feature (configured with the **crypto ipsec** command) is supported in software only for administrative connections to Catalyst 6500 series switches. | | | X | | X |
| MPLS | | | X | | X |
| IPsec VPNs | | | X | | X |

| Feature Name | IP Base | IP Services | Advanced IP Services | Enterprise Services | Advanced Enterprise Services |
|---|---|---|---|---|---|
| ISO CLNS | | | | X | X |
| Novell IPX | | | | X | X |
| IPv6 | | | | | |
| With releases earlier than Release 12.2(33)SXI: | | | X | X | X |
| With Release 12.2(33)SXI and later releases: | X | X | X | X | X |
| Cisco IOS server load balancing (SLB) | | X | X | X | X |
| IS-IS | | | X | X | X |
| VSS | | | | | |
| With releases earlier than Release 12.2(33)SXI1: | | X | X | X | X |
| With Release 12.2(33)SXI1 and later releases: | X | X | X | X | X |
| BGP4 | | X | X | X | X |
| MBGP | | X | X | X | X |
| VRF Lite | | X | X | X | X |
| Bidirectional PIM | | X | X | X | X |
| EIGRP | | X | X | X | X |
| MSDP | | X | X | X | X |
| OSPF<br>**Note** CSCth76325 prevents support of OSPFv2 in IOS IP Base images in Release 12.2(33)SXI4. Release 12.2(33)SXI4 Software Modularity IP Base images support OSPFv2. | X | X | X | X | X |
| PBR | | X | X | X | X |
| NetFlow | X | X | X | X | X |
| EIGRP Stub Routing | X | X | X | X | X |
| HSRP | X | X | X | X | X |
| IGMP | X | X | X | X | X |
| IPsec Triple DES Encryption (3DES) for SSH<br>**Note** The SSH k9 images support SSH 3DES access in software on the route processor. | X | X | X | X | X |
| PIMv1, PIMv2 | X | X | X | X | X |
| RIPv1, RIPv2 | X | X | X | X | X |

# New Features


- New Features in Release 12.2(33)SXJ6, page 118
- New Features in Release 12.2(33)SXJ5, page 118
- New Features in Release 12.2(33)SXJ4, page 119
- New Features in Release 12.2(33)SXJ3, page 119

- New Features in Release 12.2(33)SXJ2, page 120
- New Features in Release 12.2(33)SXJ1, page 121
- New Features in Release 12.2(33)SXJ, page 123
- New Features in Release 12.2(33)SXI12, page 124
- New Features in Release 12.2(33)SXI11, page 125
- New Features in Release 12.2(33)SXI10, page 125
- New Features in Release 12.2(33)SXI9, page 126
- New Features in Release 12.2(33)SXI8a, page 126
- New Features in Release 12.2(33)SXI8, page 126
- New Features in Release 12.2(33)SXI7, page 127
- New Features in Release 12.2(33)SXI6, page 127
- New Features in Release 12.2(33)SXI5, page 128
- New Features in Release 12.2(33)SXI4a, page 128
- New Features in Release 12.2(33)SXI4, page 128
- New Features in Release 12.2(33)SXI3, page 131
- New Features in Release 12.2(33)SXI2a, page 131
- New Features in Release 12.2(33)SXI2, page 131
- New Features in Release 12.2(33)SXI1, page 133
- New Features in Release 12.2(33)SXI, page 133
- New Features in Release 12.2(33)SXH8b, page 142
- New Features in Release 12.2(33)SXH8a, page 143
- New Features in Release 12.2(33)SXH8, page 143
- New Features in Release 12.2(33)SXH7, page 143
- New Features in Release 12.2(33)SXH6, page 144
- New Features in Release 12.2(33)SXH5, page 144
- New Features in Release 12.2(33)SXH4, page 145
- New Features in Release 12.2(33)SXH3a, page 145
- New Features in Release 12.2(33)SXH3, page 146
- New Features in Release 12.2(33)SXH2a, page 146
- New Features in Release 12.2(33)SXH2, page 146
- New Features in Release 12.2(33)SXH1, page 147
- New Features in Release 12.2(33)SXH, page 148
- Software Features from Earlier Releases, page 163

**Note**

- See the "Supervisor Engine 32 (CAT6000-SUP32/MSFC2A)" section on page 22 for the list of features not supported with Supervisor Engine 32.
- Cisco ME 6500 Series Ethernet switches (ME6524) are not supported in Release 12.2(33)SXJ and later releases. Support continues in Release 12.2(33)SXI and rebuilds.
- See the following site for information about MIBs:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- Features in the Cisco IOS 12.2SX releases that are also supported in the Cisco IOS 12.2 mainline, 12.2T and 12.2S releases are documented in the publications for those releases. When applicable, this section refers to those publications for platform-independent features supported in the Cisco IOS 12.2SX releases.
- Release 12.2(33)SXJ and later releases support NTPv4. Earlier releases support NTPv3. With NTPv3, be aware of CSCec87418.

# New Features in Release 12.2(33)SXJ6

These sections describe the new features in Release 12.2(33)SXJ6, 23 Jul 2013:


- New Hardware Features in Release 12.2(33)SXJ6, page 118
- New Software Features in Release 12.2(33)SXJ6, page 118


## New Hardware Features in Release 12.2(33)SXJ6

None.

## New Software Features in Release 12.2(33)SXJ6

- IP Access List Entry - Persistent Sequence Numbering Across Reloads—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/12-2sx/sec-acl-seq-num-persistent.html

# New Features in Release 12.2(33)SXJ5

These sections describe the new features in Release 12.2(33)SXJ5, 08 Feb 2013:


- New Hardware Features in Release 12.2(33)SXJ5, page 118
- New Software Features in Release 12.2(33)SXJ5, page 119


## New Hardware Features in Release 12.2(33)SXJ5

None.

## New Software Features in Release 12.2(33)SXJ5

None.

# New Features in Release 12.2(33)SXJ4

These sections describe the new features in Release 12.2(33)SXJ4, 31 Aug 2012:


- New Hardware Features in Release 12.2(33)SXJ4, page 119
- New Software Features in Release 12.2(33)SXJ4, page 119


## New Hardware Features in Release 12.2(33)SXJ4

None.

## New Software Features in Release 12.2(33)SXJ4

Configurable System Controller Reset Threshold—With a redundant supervisor engine, if a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, the affected supervisor engine reloads.

Without a redundant supervisor engine, if a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, one of the following happens:

- If the system controller reset threshold has not been reached, reset the system controller ASIC.
- If the system controller reset threshold has been reached, reload the supervisor engine.

The default system controller reset threshold value is 1, configurable with the **platform system-controller reset-threshold** *threshold_value* command. The value range is 1 through 100.

TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, and TM_NPP_PARITY_ERROR errors cause system messages.

- Before the threshold is reached, the errors cause the following system messages:

  %SYSTEM_CONTROLLER-<>-THRESHOLD
  %SYSTEM_CONTROLLER-<>-ERROR
  %SYSTEM_CONTROLLER-<>-MISTRAL_RESET

- After the threshold is reached, the errors cause the following system messages:

  %SYSTEM_CONTROLLER-<>-ERROR
  %SYSTEM_CONTROLLER-<>-FATAL

# New Features in Release 12.2(33)SXJ3

These sections describe the new features in Release 12.2(33)SXJ3, 25 Apr 2012:


- New Hardware Features in Release 12.2(33)SXJ3, page 120
- New Software Features in Release 12.2(33)SXJ3, page 120

**Note** IOS Server Load Balancing (SLB) is not supported in Release 12.2(33)SXJ and later releases. Support continues in Release 12.2(33)SXI and rebuilds. Release 12.2(33)SXJ and later releases support server load balancing (SLB) as implemented on the Application Control Engine (ACE) module (ACE20-MOD-K9). The IOS SLB CLI is not present in Release 12.2(33)SXJ3 and later releases.

### New Hardware Features in Release 12.2(33)SXJ3

None.

### New Software Features in Release 12.2(33)SXJ3

None.

## New Features in Release 12.2(33)SXJ2

These sections describe the new features in Release 12.2(33)SXJ2, 19 Dec 2011:


- New Hardware Features in Release 12.2(33)SXJ2, page 120
- New Software Features in Release 12.2(33)SXJ2, page 120


**Note** In Release 12.2(33)SXJ2 and later releases, syslog messages are generated if the clock source on packet-over-sonet interfaces changes because of an alarm on the link or if an S1 synchronization status message byte (SSB) is received. Clock source changes caused by command entry do not generate syslog messages. (CSCtk10010)

### New Hardware Features in Release 12.2(33)SXJ2

None.

### New Software Features in Release 12.2(33)SXJ2

- PoE Plus (PoE+, PoEP) support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/power_over_ethernet.html#PoE_Plus_(PoE+,_PoEP)_support

- Port Channel Load Deferral—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Configuring_Port_Load_Share_Deferral_on_the_Peer_Switch

- VPLS PIM and IGMP Snooping (WAN Interfaces)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snooigmp.html#VPLS_PIM_and_IGMP_Snooping_(WAN_Interfaces)

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snooppim.html#VPLS_PIM_and_IGMP_Snooping_(WAN_Interfaces)

- LLDP Inline Power Negotiation for PoE+—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/power_over_ethernet.html#LLDP_Inline_Power_Negotiation_for_PoE+

# New Features in Release 12.2(33)SXJ1

These sections describe the new features in Release 12.2(33)SXJ1, 30 Jun 2011:


- New Hardware Features in Release 12.2(33)SXJ1, page 121
- New Software Features in Release 12.2(33)SXJ1, page 121


**Note** In Release 12.2(33)SXJ1 and later releases, CDP is disabled by default on ES+ line card and 7600-SIP-600 ports (CSCtk12860).

## New Hardware Features in Release 12.2(33)SXJ1

- ASA Services Module for Catalyst 6500-E, 3DES/AES (WS-SVC-ASA-SM1-K9)

  **Note** Supported only with 6500 E-series chassis: WS-C6513-E, WS-C6509-V-E, WS-C6509-E, WS-C6506-E, WS-C6504-E, and WS-C6503-E. Not supported in PFC3A mode.

- Network Analysis Module 3 (WS-SVC-NAM3-6G-K9)

  **Note** Supported only with 6500 E-series chassis: WS-C6513-E, WS-C6509-V-E, WS-C6509-E, WS-C6506-E, WS-C6504-E, and WS-C6503-E. Not supported in PFC3A mode.

- Four-port Ethernet Services Plus Extended Transport (ES+XT) Line Cards (76-ES+XT-4TG3CXL, 76-ES+XT-4TG3C)
- Two-port Ethernet Services Plus Extended Transport (ES+XT) Line Cards (76-ES+XT-2TG3CXL, 76-ES+XT-2TG3C)
- Four-port Ethernet Services Plus (ES) Line Cards (7600-ES+4TG3CXL, 7600-ES+4TG3C)
- Two-port Ethernet Services Plus (ES) Line Card (7600-ES+2TG3CXL, 7600-ES+2TG3C)
- 10GBASE-LR 1310 nm SMF (SFP-10G-LR)
- 10GBASE-T X2 Module for CAT6A/CAT7 copper cable (X2-10GB-T)

## New Software Features in Release 12.2(33)SXJ1

- 6500 ES+XT-4TG3C/3CXL support with VSS—The ES+ line cards are supported in VSS mode.
- Critical voice VLAN support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Critical_voice_VLAN_support

- IGMP snooping querier enhancements—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snooigmp.html#IGMP_snooping_querier_enhancements

- IPSec Encryption in VSS System—VSS mode supports the WS-SSC-600 Services SPA Carrier (SSC) and WS-IPSEC-3 IPsec SPA.
- IPv6 Route Health Injection (IPv6 RHI) on ACE-30—Release 12.2(33)SXJ1 provides support on the switch for the IPv6 RHI feature implemented on the ACE30-MOD-K9.
- Routed Pseudo-Wire and Routed VPLS—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/l2vpn_advanced_vpls.html#Routed_Pseudo-Wire_and_Routed_VPLS
- VLAN translation support with A-VPLS—Release 12.2(33)SXJ1 testing verified support for L2VPN Advanced VPLS (A-VPLS) traffic through ES+ line ports and through LAN ports configured for VLAN translation.
- VRF aware source interface for syslog transactions—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_09.html#logging_source-interface

  http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_09.html#logging_source-interface
- VRF-lite aware NAT for non-overlapping IP addresses:

**Note** NAT VRF-lite is supported **only** with nonoverlapping IP addresses.

The following is an example of the supported configuration:

```
ip nat outside source static real_ip_address nat_ip_address

interface vlan vlan_ID_X
  ip nat inside
  ip vrf forwarding vrf_name
  ip address vrf_ip_add mask_value

interface vlan vlan_ID_Y
  ip nat outside
  ip vrf forwarding vrf_name
  ip address vrf_ip_add mask_value
! Configuration of up to 248 interfaces supported.
!
ip nat inside source static local_ip1 global_ip1 vrf vrf_name
ip nat inside source static local_ip2 global_ip2 vrf vrf_name
!
! Up to 124 of these statements
```

**Note**

- This feature is not supported if there are overlaping IP address ranges among the VRF-lite domains. Support for this feature is limited to VRF-lite configurations with non-overlapping IP addresses.
- This feature has limited support based on the provided sample configuration.

# New Features in Release 12.2(33)SXJ

These sections describe the new features in Release 12.2(33)SXJ, 21 Mar 2011:


- New Hardware Features in Release 12.2(33)SXJ, page 123
- New Software Features in Release 12.2(33)SXJ, page 123


**Note**

- Cisco ME 6500 Series Ethernet switches (ME6524) are not supported in Release 12.2(33)SXJ and later releases. Support continues in Release 12.2(33)SXI and rebuilds.
- IOS Server Load Balancing (SLB) is not supported in Release 12.2(33)SXJ and later releases. Support continues in Release 12.2(33)SXI and rebuilds. Release 12.2(33)SXJ and later releases support server load balancing (SLB) as implemented on the Application Control Engine (ACE) module (ACE20-MOD-K9).

## New Hardware Features in Release 12.2(33)SXJ

- Wireless Services Module 2 (WiSM2) (WS-SVC-WISM2-K9)—See the "Wireless Services Module 2 (WiSM2)" section on page 99.
- 5-port Gigabit Ethernet SPA, SFP Optics, version 2 (SPA-5X1GE-V2)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76intsw.html#SIP,_SSC,_and_SPA_Compatibility

**Note** Release 12.2(33)SXJ and later releases do not support these modules:

- Content Switching Module (CSM; WS-X6066-SLB-APC)
- Content Switching Module with SSL (CSM-S; WS-X6066-SLB-S-K9)
- Secure Sockets Layer (SSL) Services Module (WS-SVC-SSL-1)

## New Software Features in Release 12.2(33)SXJ

**Note** Release 12.2(33)SXJ and later releases do not support Cisco IOS Software Modularity. With redundant supervisor engines, eFSU upgrade from a Cisco IOS Software Modularity image to a Release 12.2(33)SXJ image might result in a significant delay before the switch becomes active; the switch will be in the RPR redundancy mode.

- eFSU (Enhanced Fast Software Upgrade) support from 12.2(33)SXI to 12.2(33)SXJ—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/issu_efsu.html#SXI_SXJ

- EnergyWise Pre Phase 2.5—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/release/notes/OL19810.html

- mLACP for Server Access—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mlacp_server_support.html

- Multi-auth Vlan Assignment—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Multi-auth_Vlan_Assignment

- NEAT (Network Edge Authentication Topology)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#NEAT_CISP

- NHRP Reformation move to IP Services—Release 12.2(33)SXJ and later releases support the next hop resolution protocol (NHRP) in the IP Services image.

- NTPv4 with support for IPv4 and IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ntpv4.html

  **Note** Release 12.2(33)SXJ and later releases support NTPv4. Earlier releases support NTPv3. With NTPv3, be aware of CSCec87418.

- NSF / SSO - Any Transport over MPLS (AToM)—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_trnsprt_mlps_atom.html

- Storm Control action -- Port disable—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/storm.html#Storm_Control_action_-_Port_disable

- Tacacs over IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-adsl_dial.html

- TrustSec VRF Aware—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/sxp_config.html

# New Features in Release 12.2(33)SXI12

These sections describe the new features in Release 12.2(33)SXI12, 13 Sep 2013:


- New Hardware Features in Release 12.2(33)SXI12, page 124
- New Software Features in Release 12.2(33)SXI12, page 124


## New Hardware Features in Release 12.2(33)SXI12

None.

## New Software Features in Release 12.2(33)SXI12

None.

# New Features in Release 12.2(33)SXI11

These sections describe the new features in Release 12.2(33)SXI11, 25 Feb 2013:


- New Hardware Features in Release 12.2(33)SXI11, page 125
- New Software Features in Release 12.2(33)SXI11, page 125


## New Hardware Features in Release 12.2(33)SXI11

None.

## New Software Features in Release 12.2(33)SXI11

None.

# New Features in Release 12.2(33)SXI10

These sections describe the new features in Release 12.2(33)SXI10, 18 Sep 2012:


- New Hardware Features in Release 12.2(33)SXI10, page 125
- New Software Features in Release 12.2(33)SXI10, page 125


## New Hardware Features in Release 12.2(33)SXI10

None.

## New Software Features in Release 12.2(33)SXI10

Configurable System Controller Reset Threshold—With a redundant supervisor engine, if a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, the affected supervisor engine reloads.

Without a redundant supervisor engine, if a TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, or TM_NPP_PARITY_ERROR error occurs, one of the following happens:

- If the system controller reset threshold has not been reached, reset the system controller ASIC.
- If the system controller reset threshold has been reached, reload the supervisor engine.

The default system controller reset threshold value is 1, configurable with the **platform system-controller reset-threshold** *threshold_value* command. The value range is 1 through 100.

TM_DATA_PARITY_ERROR, TM_LINK_ERR_INBAND, and TM_NPP_PARITY_ERROR errors cause system messages.

- Before the threshold is reached, the errors cause the following system messages:

  %SYSTEM_CONTROLLER-<>-THRESHOLD
  %SYSTEM_CONTROLLER-<>-ERROR
  %SYSTEM_CONTROLLER-<>-MISTRAL_RESET

- After the threshold is reached, the errors cause the following system messages:

  %SYSTEM_CONTROLLER-<>-ERROR
  %SYSTEM_CONTROLLER-<>-FATAL

# New Features in Release 12.2(33)SXI9

These sections describe the new features in Release 12.2(33)SXI9, 02 Mar 2012:


- New Hardware Features in Release 12.2(33)SXI9, page 126
- New Software Features in Release 12.2(33)SXI9, page 126


## New Hardware Features in Release 12.2(33)SXI9

None.

## New Software Features in Release 12.2(33)SXI9

None.

# New Features in Release 12.2(33)SXI8a

These sections describe the new features in Release 12.2(33)SXI8a, 07 Dec 2011:


- New Hardware Features in Release 12.2(33)SXI8a, page 126
- New Software Features in Release 12.2(33)SXI8a, page 126


## New Hardware Features in Release 12.2(33)SXI8a

None.

## New Software Features in Release 12.2(33)SXI8a

None.

# New Features in Release 12.2(33)SXI8

These sections describe the new features in Release 12.2(33)SXI8, 03 Nov 2011:


- New Hardware Features in Release 12.2(33)SXI8, page 126
- New Software Features in Release 12.2(33)SXI8, page 126


## New Hardware Features in Release 12.2(33)SXI8

None.

## New Software Features in Release 12.2(33)SXI8

- Port Channel Load Deferral—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Configuring_Port_Load_Share_Deferral_on_the_Peer_Switch

# New Features in Release 12.2(33)SXI7

These sections describe the new features in Release 12.2(33)SXI7, 26 Jul 2011:


- New Hardware Features in Release 12.2(33)SXI7, page 127
- New Software Features in Release 12.2(33)SXI7, page 127


## New Hardware Features in Release 12.2(33)SXI7

None.

## New Software Features in Release 12.2(33)SXI7

- Enhanced IPv6 Neighbor Discovery Cache Management—See this publication:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-addrg-bsc-con.html

# New Features in Release 12.2(33)SXI6

These sections describe the new features in Release 12.2(33)SXI6, 31 Mar 2011:


- New Hardware Features in Release 12.2(33)SXI6, page 127
- New Software Features in Release 12.2(33)SXI6, page 127


## New Hardware Features in Release 12.2(33)SXI6

None.

## New Software Features in Release 12.2(33)SXI6

- VRF-lite aware NAT for non-overlapping IP addresses:

**Note** NAT VRF-lite is supported **only** with nonoverlapping IP addresses.

The following is an example of the supported configuration:

```
ip nat outside source static real_ip_address nat_ip_address

interface vlan vlan_ID_X
  ip nat inside
  ip vrf forwarding vrf_name
  ip address vrf_ip_add mask_value

interface vlan vlan_ID_Y
  ip nat outside
  ip vrf forwarding vrf_name
  ip address vrf_ip_add mask_value
! Configuration of up to 248 interfaces supported.
!
ip nat inside source static local_ip1 global_ip1 vrf vrf_name
ip nat inside source static local_ip2 global_ip2 vrf vrf_name
```

```
!
! Up to 124 of these statements
```

**Note**

- This feature is not supported if there are overlaping IP address ranges among the VRF-lite domains. Support for this feature is limited to VRF-lite configurations with non-overlapping IP addresses.
- This feature has limited support based on the provided sample configuration.

# New Features in Release 12.2(33)SXI5

These sections describe the new features in Release 12.2(33)SXI5, 29 Oct 2010:


- New Hardware Features in Release 12.2(33)SXI5, page 128
- New Software Features in Release 12.2(33)SXI5, page 128


## New Hardware Features in Release 12.2(33)SXI5

None.

## New Software Features in Release 12.2(33)SXI5

- NAT - Routemaps Outside-to-Inside support (supported only on ME 6500 switches)—See this document:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/12-2sx/iadnat-addr-consv.html

# New Features in Release 12.2(33)SXI4a

These sections describe the new features in Release 12.2(33)SXI4a, 22 Jul 2010:


- New Hardware Features in Release 12.2(33)SXI4a, page 128
- New Software Features in Release 12.2(33)SXI4a, page 128


## New Hardware Features in Release 12.2(33)SXI4a

None.

## New Software Features in Release 12.2(33)SXI4a

None.

# New Features in Release 12.2(33)SXI4

These sections describe the new features in Release 12.2(33)SXI4, 09 Jun 2010:


- New Hardware Features in Release 12.2(33)SXI4, page 129
- New Software Features in Release 12.2(33)SXI4, page 129

**Note** CSCth76325 prevents support of OSPFv2 in IOS IP Base images in Release 12.2(33)SXI4. Release 12.2(33)SXI4 Software Modularity IP Base images support OSPFv2.

## New Hardware Features in Release 12.2(33)SXI4

- 16-Port 10 Gigabit Ethernet Copper Module (WS-X6716-10T-3C, WS-X6716-10T-3CXL)
- 48-port 10/100/1000 Mbps (WS-X6148E-GE-45AT)
- 7600-SIP-400 support in VSS mode
- Application Control Engine (ACE) module (ACE30-MOD-K9)
- Secure Sockets Layer (SSL) Services Module (WS-SVC-SSL-1)
- 10GBASE-LRM 1310 nm MMF and SMF (SFP-10G-LRM)

## New Software Features in Release 12.2(33)SXI4

- Auto Interleaved Port priority for LACP—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/channel.html
- DHCP - Server Port Based Address Allocation—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-2sx/dhcp-prt-bsd-aa.html
- Energywise Phase - 2—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/configuration/guide/ew_v2.html
- Fast UDLD—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/udld.html
- HSRP: Global IPv6 Address—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-fhrp.html
- IEEE 802.1x - RADIUS Change of Authorization (CoA)—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authentifcn.html
- IPv6 PACL support—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- IPv6 Policy-Based Routing—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-pol-bsd-rtng.html
- IPv6 RA-Guard Host Mode—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- L2VPN Advanced VPLS (A-VPLS)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/l2vpn_advanced_vpls.html
- Mac Move and Replace—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Understanding_MAC_Move

- MPLS - Egress Netflow—See this publication:

  http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/cfg_nf_egress_acctg.html

- Multicast Service Reflection—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_serv_reflect.html

- Netflow Data Export to a collector in a VRF—See this publication:

  http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_01.html#ip_flow-export_destination

- NSF/SSO - Virtual Private LAN Services (supported only on 7600-SIP-400 ports)—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpls_atom.html

- OSPF for Routed Access—OSPF for Routed Access OSPF for routed access is designed specifically to enable customers to extend Layer 3 routing capabilities to the access or Wiring Closet. OSPF for routed access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes. With the typical topology (hub and spoke) in a campus environment, where the wiring closets (spokes) are connected to the distribution switch (hub) forwarding all nonlocal traffic to the distribution layer, the wiring closet switch need not hold a complete routing table. In your best practice design, the distribution switch sends a default route to the wiring closet switch to reach inter-area and external routes (OSPF stub or totally stub area configuration). Refer to the following link for more details:

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html

  The IP Base image supports OSPF for routed access. The IP Services image is required if you need multiple OSPFv2 and OSPFv3 instances without route restrictions. Additionally, IP Services is required to enable the VRF-lite feature.

  **Note** CSCth76325 prevents support of OSPFv2 in IOS IP Base images in Release 12.2(33)SXI4. Release 12.2(33)SXI4 Software Modularity IP Base images support OSPFv2.

- Service Advertisement Framework (SAF)—See this publication:

  http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/saf_cg.html

- SIP 400 Support on VSS—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html

- TrustSec IPv6 SGT Learning from Data-Path—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

- TrustSec SXP SNMP and Syslogs—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

- VPLS MAC Address Withdrawal—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_hvpls_npe_red.html

- VSS Quad-Sup Uplink Forwarding—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html

- VSS VSL Multicast Fast Redirect—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html

# New Features in Release 12.2(33)SXI3

These sections describe the new features in Release 12.2(33)SXI3, 04 Nov 2009:


- New Hardware Features in Release 12.2(33)SXI3, page 131
- New Software Features in Release 12.2(33)SXI3, page 131


## New Hardware Features in Release 12.2(33)SXI3

None.

## New Software Features in Release 12.2(33)SXI3

- Deprecation of install mode and patching with Cisco IOS Software Modularity—See this publication:

  http://www.cisco.com/en/US/docs/ios/swmod/configuration/guide/sw_mod_instl_cfg.html

- LACP Port-Channel Standalone Disable—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-o1.html#GUID-7D465C5C-2593-4210-8F99-F06E889F1019

# New Features in Release 12.2(33)SXI2a

These sections describe the new features in Release 12.2(33)SXI2a, 03 Sep 2009:


- New Hardware Features in Release 12.2(33)SXI2a, page 131
- New Software Features in Release 12.2(33)SXI2a, page 131


## New Hardware Features in Release 12.2(33)SXI2a

None.

## New Software Features in Release 12.2(33)SXI2a

None.

# New Features in Release 12.2(33)SXI2

These sections describe the new features in Release 12.2(33)SXI2, 17 Jul 2009:


- New Hardware Features in Release 12.2(33)SXI2, page 132
- New Software Features in Release 12.2(33)SXI2, page 132

## New Hardware Features in Release 12.2(33)SXI2

- Content Switching Module (CSM)—See these websites:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/tsd_products_support_model_home.html

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/index.html
- Content Switching Module with SSL (CSM-S)—See these websites:

  http://www.cisco.com/en/US/products/ps6077/tsd_products_support_model_home.html

  http://www.cisco.com/en/US/products/ps6077/index.html
- OneX 10G X2 to SFP+ Converter (CVR-X2-SFP10G)
- 1-Port 10 Gigabit Ethernet SPA (SPA-1X10GE-L-V2)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76intsw.html#SIP,_SSC,_and_SPA_Compatibility

## New Software Features in Release 12.2(33)SXI2

- 802.1ag - IEEE D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/12-2sy/ce-cfm-ieee-y1731.html
- Automated Notification and Detection of LTL/FPOE Problem—The Local Target Logic and Fabric Port Of Exit Static Random Access Memory in various constellation based cards are not protected via Empty Catch Clause. A software based parity table is now maintained and updated in firmware to detect and recover from Static Random Access Memory errors on LAN and Komodo+ cards.
- Filter-ID Based ACL Application—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Filter-ID_ACLs
- Local forwarding on Standby Supervisor Uplinks—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-f1.html#GUID-A815D749-F21A-4624-9DCB-81390BBE369E
- SSO - BFD—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html
- SSO - Etherchannel Traffic Convergence Improvement—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/nsfsso.html#Redundancy_Configuration_Guidelines_and_Restrictions
- Subinterface Crypto connect vlan support for E-Flexwan/FE PA—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76ovwvpn.html#Interoperability
- VSS - MPLS/IPv6 Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Software_Features

# New Features in Release 12.2(33)SXI1

These sections describe the new features in Release 12.2(33)SXI1, 31 Mar 2009:


- New Hardware Features in Release 12.2(33)SXI1, page 133
- New Software Features in Release 12.2(33)SXI1, page 133


## New Hardware Features in Release 12.2(33)SXI1

None.

## New Software Features in Release 12.2(33)SXI1

**Note** See the following site for information about supported MIBs:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- 6PE Multipath—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mptcl-bgp.html
- 802.1x with user distribution—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_Multiple_VLANs_and_VLAN_User_Distribution_with_VLAN_Assignment
- BGP Support for 4-byte ASN—See these publications:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_basic_net.html
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_overview.html
- CISCO-IP-IF-MIB Support for IP Helper addresses—See this publication:

  http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_iptunnelmibs.html
- Modular IOS Usability - ION Installer Usability Enhancements—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/swmod/configuration/12-2sx/sm-12-2sx-book.html
- Trusted boundary with Cisco device verification—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/qos.html#Configuring_Trusted_Boundary_Device_Verification
- VSS Support on IP Base Image—See the "Feature Set Descriptions" section on page 115.

# New Features in Release 12.2(33)SXI

These sections describe the new features in Release 12.2(33)SXI, 11 Nov 2008:


- New Hardware Features in Release 12.2(33)SXI, page 134
- New Software Features in Release 12.2(33)SXI, page 135

**Note**

- Release 12.2(33)SXJ and later releases support NTPv4. Earlier releases support NTPv3. With NTPv3, be aware of CSCec87418.
- These comands, which are present in the Release 12.2(33)SXI CLI, will be tested and supported in a future release:
  - **add prepend** option to **install bind command**
  - **add reload** option to **install activate command**
  - **add pending** option to **show install running command**
  - **mls qos trust device cisco-phone** (CSCsv53392)
- NAC Layer 3 IP validation, called "NAC - Network Admission Control" in Feature Navigator, is supported only in Release 12.2(33)SXH and rebuilds. Release 12.2(33)SXI and later releases do not support NAC Layer 3 IP validation.
- With Release 12.2(33)SXI and later releases where CSCso97991 is not resolved, you must configure an appropriate burst size when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.
- Release 12.2(33)SXI and later releases support additional logical interfaces (see the "Spanning Tree Troubleshooting" section on page 9).

## New Hardware Features in Release 12.2(33)SXI

- 10GBASE DWDM X2 Modules—See this publication:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6576/data_sheet_c78_489725.html
- 10GBASE-ZR X2 Module for SMF (X2-10GB-ZR)—See this publication:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6574/product_data_sheet0900aecd801f92aa_ps5251_Products_Data_Sheet.html
- 2-Port Gigabit Ethernet Shared Port Adapter (SPA-2X1GE-V2)
- ATM SPAs:
  - 1-Port OC-12c/STM-4c ATM SPA (SPA-1XOC12-ATM)
  - 1 port OC-48c/STM-16 ATM SPA (SPA-1XOC48-ATM)
  - 2-Port OC-3c/STM-1c ATM SPA (SPA-2XOC3-ATM, SPA-4XOC3-ATM)
  - 2-Port OC-48 POS/RPR SPA (2xOC48 POS/RPR SPA)
  - See these publications:

    http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76ovwpos.html

    http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/6500series/6500sov.html

- Services SPA Carrier-600 (WS-SSC-600) and VPN Services Port Adapter (WS-IPSEC-3)—See these publications:

  http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/configuration/guide/ivmsw_book.html

  http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/hardware/ivmhw_book.html

## New Software Features in Release 12.2(33)SXI

**Note** See the following site for information about supported MIBs:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- Asymmetric Carrier Delay—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgsip.html#Configuring_Asymmetric_Carrier_Delay

- AToM over GRE - Phase 2—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgeth.html#Configuring_AToM_over_GRE

- Backplane Traffic Monitor—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/plat_mon.html

- Bandwidth-Based Call Admission Control (CAC) for IP Multicast—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_admission_control.html

- BGP Route-Map Continue Support for Outbound Policy—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_external_sp.html

- Callhome Request—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/callhome.html#Sending_a_Request_for_an_Analysis_and_Report

- CatOS Parity: Port VLAN Granularity for Show Commands—See these publications:

  http://www.cisco.com/en/US/docs/ios-xml/ios/cether/command/ce-s1.html#GUID-E84B167B-7119-4921-8A62-3664F5F3F144

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s4.html#GUID-C5A646B9-2364-4412-93EF-AF21D42470BD

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s4.html#GUID-9B5E979A-69F9-41B5-9EDC-26717977DC03

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s4.html#GUID-2EE37145-597D-40E1-9E5F-EA466D7CD656

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s4.html#GUID-499A9431-66B6-4001-AD4F-BD02B04731E3

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s4.html#GUID-96B5F041-14B6-44A3-9624-F1569F4B1E91

http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s5.html#GUID-5932AC84-8527-4F41-8FE1-4EC1D7B61806

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_10.html#show_cdp

- CDP Enhancement - Host presence TLV—See these publications:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#802.1X_Host_Modes

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/voip.html#Cisco_IP_Phone_Data_Traffic

- CFM-2—See this publication:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm.html

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_metro_ethernet.html

- CNS—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html

- CNS - Configuration Agent—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html

- CNS - Event Agent—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html

- CNS - Image Agent—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html

- CNS - Interactive CLI—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html

- Command Scheduler (Kron)—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html

- Config Change Tracking Identifier— The Config Change Tracking Identifier feature assigns a version number to each saved version of the Cisco IOS running-config file and displays details about the versions. When the version number is updated a notification is generated. The Config Logger can also use this feature to determine if there have been any changes to the Cisco IOS running-config file. To enable the Config Change Tracking Identifier feature, enter the **show config id command**.

- Configuration Rollback Confirmed Change—See this publication:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-rollback.html

- DHCP - DHCPv6 Relay Agent notification for Prefix Delegation—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-dhcp.html

- DHCPv6 - Relay - Reload persistent Interface ID option—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-dhcp.html

- DHCPv6 Ethernet Remote ID option—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-dhcp.html

- Display Admin speed/duplex negotiation status—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/intrface.html#Displaying_the_Speed_and_Duplex_Mode_Configuration

- Dual PQ (Priority Queue)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgsip.html#Configuring_Dual_Priority_Queuing_on_a_Cisco_7600_SIP-400

- eFSU (Enhanced Fast Software Upgrade)—See these publications:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/issu_efsu.html

- Embedded Event Manager (EEM) 2.4—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html

- Embedded Syslog Manager (ESM)—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_esm_syslog.html

- Ethernet Local Management Interface (LMI) at Provider Edge (PE)—See these publications:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_elmi-pe.html

  http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htethlmi.html

- Ethernet OAM-phase2/ELMI-PE—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgeth.html#Configuring_Ethernet_Operations,_Administration,_and_Maintenance

- FHRP - EOT integration with EEM—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-4t/iap-eot.html

- FHRP - GLBP Client Cache—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-glbp.html

- FHRP - GLBP Support for IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-fhrp.html

- FHRP - HSRP Group Shutdown—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-hsrp.html

- FHRP - HSRP Multiple Group Optimization—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-hsrp.html

- Flash MIB enhancements—The Flash MIB Enhancements feature allows sorting of flash files according to device, partition, and file indexes. Beginning with Cisco IOS Release 12.2(33)SXI, the Flash MIB Enhancements feature adds the user functionality to sort flash files based on file type. The feature also introduces the **snmp mib flash cache interval** command to set the frequency of the data collection process that enables sorting of data stored in ciscoFlashFileTable. The command also enables the cache for ciscoFlashFileTable to speed up access to data. For more information about setting the data collection interval, see the **snmp mib flash cache interval** command in the Cisco IOS Network Management Command Reference at the following URL:

  http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

  To locate and download the Cisco Flash MIB for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

  http://tools.cisco.com/ITDIT/MIBS/servlet/index

- HSRP for IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-fhrp.html

- HSRP Gratuitous ARP—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-hsrp.html

- IEEE 802.1ak - MVRP and MRP—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/IEEE802_1ak_MVRP_MRP.html

- IEEE 802.1X - Flexible Authentication—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/dot1x_flex_auth.html

- IEEE 802.1X - Multiple Authentication—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Multiauthentication_Mode

- IEEE 802.1X - Open Authentication—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Pre-Authentication_Open_Access

- IEEE 802.1X - User Port Description—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Port_Descriptors

- IEEE 802.1X Agentless Audit Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#NAC_Agentless_Audit_Support

- IEEE 802.1x Fallback support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Understanding_the_Port-based_Authentication_Process

- IEEE 802.1X Multi-Domain Authentication—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Multidomain_Authentication_Mode

- IEEE 802.1x with ACL Assignments—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_ACL_Assignments_and_Redirect_URLs

- IEEE 802.3ah - Link Fault RFI Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_oam.html

- Intrusion Detection Service Module (IDSM) support in VSS mode—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Service_Module_Support

- IP SLAs for Metro-Ethernet—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_metro_ethernet.html

- IP SLAs Random Scheduler—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_multi_scheduler.html

- IPv6 Access Services: DHCPv6 Relay Agent—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-dhcp.html

- IPv6 ACL Extensions for Mobile IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mobile.html
- IPv6 Reformation—IPv6 features are supported in ipbase(k9) and ipservices(k9) images.
- IPv6 Routing - EIGRP Support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-eigrp.html
- IPv6 support for VSPA, VPN Services Port Adapter (WS-IPSEC-3)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/configuration/guide/ivmvpn3.html
- IPv6 VPN over MPLS (6VPE)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-ov-mpls-6vpe.html
- IPv6: Multicast Address Group Range Support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- L2VPN Pseudowire Redundancy—See this publication:

  http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_l2vpn_pw_red.html
- LowSpeed SPA support on SIP400—See these publications:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76ovwser.html#Release_History

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/6500series/6500sov.html
- MAC Move Counters—See this publication:

  http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_m1.html#mac-address-table_notification_mac-move
- Mini Protocol Analyzer—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mpa.html
- MPLS EM - LSP Ping/Trace for LDP & RSVP IPv4 FECs—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_te_lsp_vccv.html
- MPLS EM - MPLS Multipath (ECMP) LSP Tree Trace—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_em_multipath_tree.html
- MPLS VPN - VRF CLI for IPv4 & IPv6 VPNs—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_ipv4_ipv6.html
- MPLS VPN 6VPE support over IP tunnels—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-ov-mpls-6vpe.html
- MPLS VPN VRF Selection using Policy Based Routing—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_vrf_select_rt.html
- MSTP PVST Simulation disabling and Peer Inconsistency Check—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/stp_enha.html#Configuring_PVST_Simulation
- Multicast Address Group Range Support—The Multicast Address Group Range Support feature enhances multicast access control by introducing the capability to define a global range of multicast groups and channels to be permitted or denied using the **ip multicast group-range** command.

- Multicast Enhancement - Egress Replication Performance Improvement for Vlan & PortChannel—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mcastv4.html#wpMulticast_Enhancement

- Multicast Replication Packet Drop Counter—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s5.html#GUID-51E19324-B9D7-4090-B49B-5003684D339F

- Netconf access for Configuration over BEEP—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_netconf.html

- NETCONF over SSHv2—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_netconf.html

- Netflow Accounting for Unicast and Multicast on GRE tunnel interface—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/12-2sx/cfg-nf-gre-tun.html

- PBF (Policy-Based Forwarding)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.html#MAC_Policy-Based_Forwarding

- Per Interface Mroute State Limit—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_admission_control.html

- Per IP Session QoS support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/qos.html#Session-Based_PFC_QoS

- Pre-encryption QOS for VSPA—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/configuration/guide/ivmvpn3.html

- QoS Statistics Enhancement—See this publication:

  http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_s4.html#show_mls_qos

- Radius Per-VRF Server Group—See this publication:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_per_vrf_aaa.html

- Rapid-PVST+ Dispute Mechanism—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/spantree.html#Rapid-PVST

- Reliable Delivery and Filtering for Syslog—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_reliable_del_filter.html

- Role-Based Access Control CLI commands—See this publication:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_role_base_cli.html

- Show Command for Interface Trap Status—Beginning with Cisco IOS Release 12.2(33)SXI, the Show Command for Interface Trap Status feature adds the **show snmp mib ifmib traps** command to display the status of linkUp and linkDown traps. For more information about viewing linkUp and linkDown trap status, see the **show snmp mib ifmib traps** command in the Cisco IOS Network Management Command Reference at the following URL:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

For more information about enabling SNMP notification types, see the Cisco IOS Network Management Configuration Guide at the following URL:

http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/12-2sx/snmp-12-2sx-book.html

- Show Diagnostic Health—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/diags.html

- SNMP over IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

- SNMPv3 - 3DES and AES Encryption Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_encrypt_snmp_sup.html

- SSO - IPv4 Multicast HA Support for Group-to-RP Mapping—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_ha_grp_to_rp_mappings.html

- SSO - VRRP—See these publications:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-vrrp.html

- Standalone MAB support—See this publication:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/standalone_mab.html

- Static Virtual Tunnel & GRE/TP interface enhancements—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfvpna.html#Configuring_an_IPSec_Virtual_Tunnel_Interface

- STP Bridge Assurance—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/stp_enha.html#Understanding_Bridge_Assurance

- Sub Millisecond Policer Burst Size Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/qos.html#wppolicer_granularity

- Syslog over IPV6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

- System Logging - EAL4 Certification Enhancements:

  **Note** Official EAL4 certification is not claimed by Cisco Systems, Inc. This feature is part of current and planned enhancements which may qualify Cisco IOS Software for future certification.

  This feature includes the following enhancements:

  - The system logging process will now generate ‘audit start’ and ‘audit stop’ messages.
  - The system logging process will now generate messages that include the date and time of an event, the type of event, the subject identity, and the outcome (success or failure) of an event.
  - Changes to logging parameters will be logged.
  - Further enhancements to minimize lost audit records.

- TACACS+ Per VRF—See this publication:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_vrf_tacas_svrs.html

- VSS - 512 Etherchannels Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Configuring_Multichassis_EtherChannels

- VSS - ACE 10/20 Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Service_Module_Support

- VSS - Dual-active detection using L2 Fast Hello detection—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Dual-Active_Detection_Using_Dual-Active_Fast_Hello_Packets

- VSS - Firewall Service Module (FWSM) support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Service_Module_Support

- VSS - PACL support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Software_Features

- VSS - Wireless (WiSM) Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Service_Module_Support

- VTP v3—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vtp.html

- Web Authentication with Critical Auth support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/webauth.html#AAA_Fail_Policy

- Webauth Enhancements—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/webauth.html#Customization_of_the_Authentication_Proxy_Web_Pages

# New Features in Release 12.2(33)SXH8b

These sections describe the new features in Release 12.2(33)SXH8b, 23 Sep 2011:


- New Hardware Features in Release 12.2(33)SXH8b, page 142
- New Software Features in Release 12.2(33)SXH8b, page 142


## New Hardware Features in Release 12.2(33)SXH8b

None.

## New Software Features in Release 12.2(33)SXH8b

None.

# New Features in Release 12.2(33)SXH8a

These sections describe the new features in Release 12.2(33)SXH8a, 23 Mar 2011:


- New Hardware Features in Release 12.2(33)SXH8a, page 143
- New Software Features in Release 12.2(33)SXH8a, page 143


## New Hardware Features in Release 12.2(33)SXH8a

None.

## New Software Features in Release 12.2(33)SXH8a

None.

# New Features in Release 12.2(33)SXH8

These sections describe the new features in Release 12.2(33)SXH8, 05 Oct 2010:


- New Hardware Features in Release 12.2(33)SXH8, page 143
- New Software Features in Release 12.2(33)SXH8, page 143


## New Hardware Features in Release 12.2(33)SXH8

None.

## New Software Features in Release 12.2(33)SXH8

None.

# New Features in Release 12.2(33)SXH7

These sections describe the new features in Release 12.2(33)SXH7, 15 Mar 2010:


- New Hardware Features in Release 12.2(33)SXH7, page 143
- New Software Features in Release 12.2(33)SXH7, page 143


## New Hardware Features in Release 12.2(33)SXH7

None.

## New Software Features in Release 12.2(33)SXH7

- VRF-lite aware NAT for non-overlapping IP addresses:

**Note** NAT VRF-lite is supported **only** with nonoverlapping IP addresses.

The following is an example of the supported configuration:

```
ip nat outside source static real_ip_address nat_ip_address

interface vlan vlan_ID_X
  ip nat inside
  ip vrf forwarding vrf_name
  ip address vrf_ip_add mask_value

interface vlan vlan_ID_Y
  ip nat outside
  ip vrf forwarding vrf_name
  ip address vrf_ip_add mask_value
! Configuration of up to 248 interfaces supported.
!
ip nat inside source static local_ip1 global_ip1 vrf vrf_name
ip nat inside source static local_ip2 global_ip2 vrf vrf_name
!
! Up to 124 of these statements
```

**Note**

- This feature is not supported if there are overlaping IP address ranges among the VRF-lite domains. Support for this feature is limited to VRF-lite configurations with non-overlapping IP addresses.
- This feature has limited support based on the provided sample configuration.

# New Features in Release 12.2(33)SXH6

These sections describe the new features in Release 12.2(33)SXH6, 21 Oct 2009:


- New Hardware Features in Release 12.2(33)SXH6, page 144
- New Software Features in Release 12.2(33)SXH6, page 144


## New Hardware Features in Release 12.2(33)SXH6

None.

## New Software Features in Release 12.2(33)SXH6

- Subinterface Crypto connect vlan support for E-Flexwan/FE PA—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76ovwvpn.html#Interoperability

# New Features in Release 12.2(33)SXH5

These sections describe the new features in Release 12.2(33)SXH5, 20 Apr 2009:


- New Hardware Features in Release 12.2(33)SXH5, page 145
- New Software Features in Release 12.2(33)SXH5, page 145

### New Hardware Features in Release 12.2(33)SXH5

None.

### New Software Features in Release 12.2(33)SXH5

None.

## New Features in Release 12.2(33)SXH4

These sections describe the new features in Release 12.2(33)SXH4, 11 Nov 2008:


- New Hardware Features in Release 12.2(33)SXH4, page 145
- New Software Features in Release 12.2(33)SXH4, page 145


### New Hardware Features in Release 12.2(33)SXH4

None.

### New Software Features in Release 12.2(33)SXH4

**Note** See the following site for information about supported MIBs:
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- Radius Per-VRF Server Group—See this publication:
  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_per_vrf_aaa.html
- TACACS+ Per VRF—See this publication:
  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_vrf_tacas_svrs.html

## New Features in Release 12.2(33)SXH3a

These sections describe the new features in Release 12.2(33)SXH3, 29 Sep 2008:


- New Hardware Features in Release 12.2(33)SXH3a, page 145
- New Software Features in Release 12.2(33)SXH3a, page 145


### New Hardware Features in Release 12.2(33)SXH3a

None.

### New Software Features in Release 12.2(33)SXH3a

None.

# New Features in Release 12.2(33)SXH3

These sections describe the new features in Release 12.2(33)SXH3, 29 Jul 2008:


- New Hardware Features in Release 12.2(33)SXH3, page 146
- New Software Features in Release 12.2(33)SXH3, page 146


## New Hardware Features in Release 12.2(33)SXH3

None.

## New Software Features in Release 12.2(33)SXH3

**Note** See the following site for information about supported MIBs:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

SSH Keyboard Interactive Authentication—See this publication:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_secure_shell_v2.html

# New Features in Release 12.2(33)SXH2a

These sections describe the new features in Release 12.2(33)SXH2a, 28 Apr 2008:


- New Hardware Features in Release 12.2(33)SXH2a, page 146
- New Software Features in Release 12.2(33)SXH2a, page 146


## New Hardware Features in Release 12.2(33)SXH2a

None.

## New Software Features in Release 12.2(33)SXH2a

None.

**Note** Resolution of CSCso05127 changed the SPAN syntax and defaults.

# New Features in Release 12.2(33)SXH2

These sections describe the new features in Release 12.2(33)SXH2, 31 Mar 2008:


- New Hardware Features in Release 12.2(33)SXH2, page 147
- New Software Features in Release 12.2(33)SXH2, page 147

## New Hardware Features in Release 12.2(33)SXH2

- 16-port 10-Gigabit Ethernet X2 Switching Module (WS-X6716-10GE)
- 6,000 W DC power supply (PWR-6000-DC)

## New Software Features in Release 12.2(33)SXH2

**Note** See the following site for information about supported MIBs:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- Cisco Enhanced PoE (ePoE) Support—Refer to this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/voip.html#wpCisco_Enhanced_PoE_Support

# New Features in Release 12.2(33)SXH1

These sections describe the new features in Release 12.2(33)SXH1, 18 Jan 2008:


- New Hardware Features in Release 12.2(33)SXH1, page 147
- New Software Features in Release 12.2(33)SXH1, page 147


## New Hardware Features in Release 12.2(33)SXH1

- Anomaly Guard Module (WS-SVC-AGM-1-K9)—See this publication:

  http://www.cisco.com/en/US/prod/collateral/modules/ps2706/end_of_life_c51-573493.html
- Traffic Anomaly Detector Module (WS-SVC-ADM-1-K9)—See this publication:

  http://www.cisco.com/en/US/prod/collateral/modules/ps2706/end_of_life_c51-573493.html

## New Software Features in Release 12.2(33)SXH1

**Note** See the following site for information about supported MIBs:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- Multi-VRF Selection Using Policy Based Routing (PBR):
  - In releases where CSCsv22779 is not resolved, Multi-VRF Selection Using PBR does not support the use of reflexive ACLs.
  - Adds hardware support for the **set ip vrf next-hop** command. Configure the **set ip vrf next-hop** command for policy based routing within the same VRF.

**Note** The **set ip next-hop** command is supported only within the global context, not within the VRF context.

  - See this publication:

    http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_mltvrf_slct_pbr.html

- VSS (Virtual Switching System):
  - Supported only with CAT6000-VS-S720-10G/MSFC3 and the hardware listed in the "Hardware Requirements" section.
  - See these publications:

    *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, Chapter 4, "Configuring Virtual Switching Systems."

    The *Cisco IOS Virtual Switch Command Reference* at:

    http://www.cisco.com/en/US/docs/ios/vswitch/command/reference/vs_book.html

**Note** In releases earlier than Release 12.2(33) SXH2, the VSS feature and the lawful intercept feature cannot be configured together. (CSCsl77715)

- VSS - Fast Link Status Notification—See the "Virtual Switching System Redundancy" section.
- VSS - GOLD in Virtual Switching System—See the "Diagnostics" section.

# New Features in Release 12.2(33)SXH

These sections describe the new features in Release 12.2(33)SXH, 20 Aug 2007:


- New Hardware Features in Release 12.2(33)SXH, page 149
- New Software Features in Release 12.2(33)SXH, page 149


**Note** Release 12.2(33)SXH provides initial support with Cisco IOS software modularity images for these service modules:

- Services SPA Carrier (SSC; 7600-SSC-400) and IPsec SPA (SPA-IPSEC-2G)
- Application Control Engine (ACE) module (ACE10-6500-K9, ACE20-6500-K9)
- Communication Media Module (WS-SVC-CMM)
- BGP Reduction in Transient Memory Usage—Cisco IOS Release 12.2(33)SXH has implemented a reduction in transient memory usage by BGP when BGP updates are built.
- Process MIB Enhancements for Software Modularity—The CISCO-PROCESS-MIB has been enhanced to support Portable Operating System Interface (POSIX) operating systems such as Cisco Software Modularity. Cisco Software Modularity images have been updated to implement the enhanced CISCO-PROCESS-MIB. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

  http://tools.cisco.com/ITDIT/MIBS/servlet/index

## New Hardware Features in Release 12.2(33)SXH

- Catalyst 6509-V-E chassis (WS-C6509-V-E)
- Supervisor Engine 720-10GE (CAT6000-VS-S720-10G/MSFC3)
- Cisco ME 6500 Series Ethernet switches (ME6524)
- 8-port 10/100 Ethernet SPA TX (SPA-8X1FE-TX-V2)
- 4-port 10/100 Ethernet SPA TX (SPA-4X1FE-TX-V2)
- 1-port Channelized STM1/OC3 to DS0 SPA (SPA-1xCHSTM1/OC3)
- Cisco 1000BASE-T NEBS 3 ESD SFP (SFP-GE-T)

## New Software Features in Release 12.2(33)SXH

**Note** See the following site for information about supported MIBs:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- ANSI TIA-1057 LLDP - MED Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_lldp-med.html
- Any Transport over MPLS (AToM): Ethernet over MPLS (EoMPLS)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/12-2sx/mp-any-transport.html

  **Note** With a Cisco ME 6500 Series Ethernet Switch (ME6524), be aware of CSCsu50427.
- Any Transport over MPLS (AToM): Graceful Restart—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_atom_grace_rstrt.html
- ATM OAM Emulation—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/12-2sx/mp-any-transport.html
- ATM Port Mode Packed Cell Relay over MPLS—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/12-2sx/mp-any-transport.html
- AutoQoS—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/auto_qos.html
- AutoRP Enhancement—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_basic_cfg.html
- AutoSecure—See these publications:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/autosec.html

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_autosecure.html

- BGP Dynamic Neighbors—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html
- BGP Multicast Inter-AS (IAS) VPN—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_cfg_mc_vpn_sup.html
- BGP Support for BFD—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_adv_features.html
- BGP Support for Dual AS Configuration for Network AS Migrations—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html
- BGP Support for Fast Peering Session Deactivation—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html
- BGP Support for IP Prefix Import from Global Table into a VRF Table—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_sup_ip_pref.html
- BGP Support for Named Extended Community Lists—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_external_sp.html
- BGP Support for Next-Hop Address Tracking—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_adv_features.html
- BGP Support for Sequenced Entries in Extended Community Lists—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_external_sp.html
- BGP Support for TCP Path MTU Discovery per Session—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html
- Bidirectional Forwarding Detection (BFD) Standard Implementation—See this publication:
  http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html
- Call Admission Control for IKE—See this publication:
  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_call_addmsn_ike.html
- Call Home—See these publications:
  http://www.cisco.com/en/US/docs/routers/7200/configuration/feature_guides/callhome_7200.html
  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/callhome.html
- Certificate - ISAKMP Profile Mapping—See this publication:
  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_isakmp_map.html
- Certificate - Storage Location Specification—See this publication:
  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_store_pki_cred.html
- Cisco IOS Login Enhancements—See these publications:
  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_login_enhance.html
  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_login_enhance.html

- Cisco IOS Scripting w/ Tcl—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/netmgmt/configuration/guide/nm_script_tcl_xe.html

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_script_tcl.html

- CLI extension to allow vlan-range for enabling or disabling mac-address learning—See this publication:

  http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_m1.html#mac-address-table_learning

- Config Logger Persistency—See this publication:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/config-logger-6149.html

- Configurable flow-creation control of acl denied flows—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/netflow.html#Configuring_Exclude_ACL-deny

- Configuration Change Notification and Logging—See this publication:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-logger.html

- Configuration Replace and Configuration Rollback—See this publication:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-rollback.html

- Consolidation of ACL Counter Values in Distributed Environment—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s6.html#GUID-1D17939B-1C8F-422C-83CE-64B096DAD13D

- Contextual Configuration Diff Utility—See this publication:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-diff.html

- Digital Optical Monitoring (DOM) Phase 2—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s4.html#GUID-73B23B10-A62E-4F88-9F4D-F37A9C14D8D8

  **Note** See this publication for additional information about DOM: http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_8031.html

- Distributed forwarding Engines (3C/3CXL) for 67xx line cards—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html

- Easy VPN Client RSA - Signature Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_easy_vpn_rsa.html

- Easy VPN Phase 5.0—See these publications:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_easy_vpn_rem.html

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_easy_vpn_srvr.html

- EasyVPN Phase 6—See this publication:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_easy_vpn_rem.html

- EIGRP Support for Route Map Filtering—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_eigrp/configuration/guide/ire_sup_route_xe.html

  http://www.cisco.com/en/US/docs/ios/iproute_eigrp/configuration/guide/ire_sup_route.html
- Embedded Event Manager (EEM) 2.3—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html
- Enhanced hot-standby Fabric switchover time—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/nsfsso.html#Redundancy_Configuration_Guidelines_and_Restrictions
- Enhanced Tracking Support / Enhanced Object Tracking / EOT—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/ipapp/configuration/guide/ipapp_eot_xe.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-4t/iap-eot.html
- Enhancing IPv6 Multicast shared-tree performance—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mcastv6.html#IPv6_Multicast_Guidelines_and_Restrictions
- Ethernet Connectivity Fault Management (E-CFM)—See this publication:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm.html
- Ethernet Operations, Administration, and Maintenance (OAM)—See these publications:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_oam.html
- Exclusive Configuration Change Access—See this publication:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-lock.html
- Extended ACL support for IGMP to support SSM in IPv4—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_customize_igmp.html
- FHRP - Enhanced Object Tracking of IP SLAs—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/ipapp/configuration/guide/ipapp_eot_xe.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-4t/iap-eot.html

  **Note** FHRP - Enhanced Object Tracking of IP SLAs is not stateful switchover (SSO)-aware and cannot be used with Hot Standby Routing Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP) in SSO mode. (CSCtd31237)
- FHRP - Object Tracking List—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-4t/iap-eot.html
- Front Side VRF—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfvpna.html#Configuring_VPNs_in_VRF_Mode
- GLBP MD5 Authentication—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-glbp.html
- GRE Tunnel IP Source and Destination VRF Membership—See this publication:

  http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_impl_tun.html

- Hardware Acceleration for Multicast VPN Extranet Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_mc_vpn_extranet.html

- HSRP MD5 Authentication—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/ipapp/configuration/guide/ipapp_hsrp_xe.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-hsrp.html

- IEEE 802.1ab LLDP (Link Layer Discovery Protocol)—See this publication:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_lldp-med.html

- IEEE 802.1Q Tagging on a Per-Port Basis—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1qtnl.html#Configuring_the_Switch_to_Tag_Native_VLAN_Traffic_Globally

- IEEE 802.1x Authenticator—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Device_Roles

- IEEE 802.1x - Auth Fail Open—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Inaccessible_Authentication_Bypass

- IEEE 802.1x - Auth Fail VLAN—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Inaccessible_Authentication_Bypass

- IEEE 802.1x Guest VLAN—See these publications:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Guest_VLAN

- IEEE 802.1x Private Guest VLAN—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Inaccessible_Authentication_Bypass

- IEEE 802.1x Private VLAN Assignment—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Configuring_a_Guest_VLAN

- IEEE 802.1x RADIUS Accounting—See these publications:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#802.1X_Accounting

- IEEE 802.1x Radius-Supplied Session Timeout—See these publications:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Enabling_Periodic_Reauthentication

- IEEE 802.1x - Voice VLAN—See these publications:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Voice_VLAN_Ports

- IEEE 802.1x - Wake on LAN Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Wake-on-LAN

- IEEE 802.1x with DHCP—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_DHCP_Snooping

- IEEE 802.1x with Port Security—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Port_Security

- IGMP Filtering—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/igmpfilt.html

- IGMP Snooping Enhancement: Global CGMP Auto-Detection—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snooigmp.html#CGMP_Automatic_Detection

- Inline power IEEE power classification override—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/voip.html#Inline_Power_Management

- IP 16-way Equal-Cost Multipath—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#maximum-paths

- IPSec Dead Peer Detection (DPD) Periodic Message Option—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_dead_peer.html

- IPSEC Preferred Peer—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_pref_peer.html

- IPSec VTI - Virtual Tunnel Interface—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_virt_tunnl.html

- IPSG (IP Source Guard)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/ipsrcgrd.html

- IP SLAs - DHCP Operation—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_dhcp.html

- IP SLAs - Distribution of Statistics—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_overview.html

- IP SLAs - DNS Operation—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_dns.html

- IP SLAs - FTP Operation—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_ftp.html

- IP SLAs - HTTP Operation—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_http.html

- IP SLAs - ICMP Echo Operation—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_icmp_echo.html
- IP SLAs - ICMP Path Echo Operation—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_icmp_pathecho.html
- IP SLAs - LSP Health Monitor—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_lsp_mon_autodisc.html
- IP SLAs - MPLS VPN Awareness—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_overview.html
- IP SLAs - Multi Operation Scheduler—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_multi_scheduler.html
- IP SLAs - One Way Measurement—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_overview.html
- IP SLAs - Path Jitter Operation—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_icmp_pathjitter.html
- IP SLAs - Reaction Threshold—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_threshold_mon.html
- IP SLAs - Scheduler—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_overview.html
- IP SLAs - TCP Connect Operation—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_tcp.html
- IP SLAs - UDP Based VoIP Operation—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_udp_jitter_voip.html
- IP SLAs - UDP Echo Operation—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_udp_echo.html
- IP SLAs - UDP Jitter Operation—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_udp_jitter.html
- IP SLAs - VoIP Threshold Traps—See this publication:
  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_threshold_mon.html
- IPv6: Anycast Address—See this publication:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-addrg-bsc-con.html
- IPv6 Default Router Preferences—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-addrg_bsc_con_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-addrg-bsc-con.html
- IPv6 Multicast: Address Family Support for Multiprotocol BGP—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- IPv6 Multicast: Explicit Tracking of Receivers—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html

http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html

- IPv6 Multicast: MLD Access Group—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- IPv6 Multicast: PIM Accept Register—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- IPv6 Multicast: PIM Embedded RP Support—See this publication:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- IPv6 Multicast: Routable Address Hello Option—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets—See this publication:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- IPv6 Multicast: Static Multicast Routing (mroute) for IPv6—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-multicast_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- IPv6 Routing: Multiprotocol BGP Extensions for IPv6—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-mptcl_bgp_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mptcl-bgp.html
- IPv6 Routing: Multiprotocol BGP Link-local Address Peering—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-mptcl_bgp_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mptcl-bgp.html
- IPv6 Routing: Route Redistribution—See these publications:
  http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-is-is_xe.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-is-is.html
- L2VPN Interworking—See this publication:
  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_l2vpn_intrntwkg.html
- L2VPN Interworking - Ethernet to VLAN Interworking—See this publication:
  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_l2vpn_intrntwkg.html
- L2VPN Interworking: Ethernet VLAN to ATM AAL5—See these publications:
  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_l2vpn_intrntwkg.html
  http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/broadband/l2vpn.html
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_and_configuration_guides_list.html
- L2VPN Interworking: Ethernet VLAN to Frame Relay—See these publications:
  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_l2vpn_intrntwkg.html
  http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/broadband/l2vpn.html

- L2VPN Interworking: Ethernet VLAN to PPP—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_l2vpn_intrntwkg.html

- L2VPN Interworking: Frame Relay to ATM AAL5—See these publications:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_l2vpn_intrntwkg.html

  http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/broadband/l2vpn.html

- L2VPN Interworking: Frame Relay to PPP—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_l2vpn_intrntwkg.html

- LACP 1-1 redundancy with fast switchover—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/channel.html#Understanding_LACP_1:1_Redundancy

- Lawful Intercept (LI)—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/sec_user_services/configuration/guide/sec_lawful_intercept_xe.html

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/lawful/intercept/book.html

  **Note** In releases earlier than Release 12.2(33)SXH2, the VSS feature and the lawful intercept feature cannot be configured together. (CSCsl77715)

- Layer 2 Local switching - ATM-FR—See these publications:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslocal.html

  http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_l2_lcl_swng.html

- Layer 2 Local Switching - ATM to Ethernet—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslocal.html

- MAC Address Notification—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/layer2.html#Configuring_MAC_Address_Table_Notification

- MAC Authentication Bypass—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_MAC_Authentication_Bypass

- Memory Pool - SNMP Notification Support—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgsip.html#Configuring_PPP_Bridging_Control_Protocol_Support

- MPLS LDP - Graceful Restart—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_grace_rstrt.html

- MPLS LDP - Session Protection—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_sessn_prot.html

- MPLS LDP - VRF Aware Static Labels—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vrf_aware_static.html

- MPLS over RBE—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgatm.html#Configuring_MPLS_over_RBE
- MPLS Static Labels—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_static_labels.html
- MPLS Traffic Engineering - AutoTunnel Mesh Groups—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_autotun_mesh.html
- MPLS Traffic Engineering - FRR Scalability Enhancements—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-frr-node-prot.html
- MPLS Traffic Engineering--Inter-AS TE—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_inter_as_te.html
- MPLS Traffic Engineering: Shared Risk Link Groups (SRLG)—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_shared_risk.html
- MPLS Traffic Engineering (TE) - AutoTunnel Primary and Backup—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_autotunnel.html
- MPLS Traffic Engineering (TE) - Class-based Tunnel Selection—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_tun_select.html
- MPLS Traffic Engineering (TE) - Fast Reroute (FRR) Link and Node Protection—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_frr_node_prot.html
- MPLS Traffic Engineering (TE) - LSP Attributes—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_lsp_attr.html
- MPLS Traffic Engineering (TE) - RSVP Hello State Timer—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_rsvp_hello.html
- MPLS Traffic Engineering (TE): Verbatim Path Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_verbatim_path.html
- MPLS VPN - Explicit Null Label Support with BGP IPv4 Label Session—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ce_vpn_explicit.html
- MPLS VPN - Loadbalancing support for Inter-AS and CSC VPNs—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_load_share_vpn.html
- MPLS VPN - Multi-Path support for Inter-AS VPNs—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_interauto.html
- MPLS VPN - Route Target Rewrite—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_rte_target_rw.html
- MPLS VPN - Show Running VRF—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_show_run_vrf.html

- MSDP compliance with IETF RFC 3618—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_msdp_im_pim_sm.html
- MSDP MD5 password authentication—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_msdp_im_pim_sm_xe.html

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_msdp_im_pim_sm.html
- Multicast Vlan Registration (MVR)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snooigmp.html#Understanding_MVR
- Multicast VPN Extranet Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_mc_vpn_extranet.html
- Multicast VPN Inter-AS Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_cfg_mc_vpn_sup.html
- Multicast VPN MIB—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_vpn_mib.html
- Multilink Frame Relay (FRF.16.1) - Variable Bandwidth Class—See this publication:

  http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_ml_fr_frf161.html
- Multi-VC to VLAN Scalability—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76ovwatm.html#SIP-Dependent_Features
- MUX UNI Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/pfc3mpls.html#Configuring_MUX-UNI_Support_on_LAN_Cards
- NAC - Auth Fail Open—See these publications:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_nat_auth_fail_op.html

  http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_nacaf.html
- NAC - L2 IEEE 802.1x—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_Network_Admission_Control_Layer_2_IEEE_802.1X_Validation
- NAC - Network Admission Control—See these publications:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_net_admssn_ctrl.html

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/nac.html
- Netflow MIB and Top Talkers—See this publication:

  http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/cfg_nflow_top_talk.html
- Netflow Multicast Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/cfg_nf_multi_acctg.html
- NetFlow Subinterface Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/cfg_nflow_data_expt.html

- NSF - OSPF (RFC 3623 OSPF Graceful Restart)—See these publications:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-mt/iro-restart.html
- NSF / SSO - MPLS LDP and LDP Graceful Restart—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_grace_nsfsso.html
- NSF/SSO - MPLS TE and RSVP Graceful Restart—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_rsvp_grace.html
- NSF/SSO - MPLS VPN—See these publications:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_nsfsso.html
- OER Border Router Only Functionality—See this publication:

  http://www.cisco.com/en/US/docs/ios/ios_xe/pfr/configuration/guide/pfr-basic_xe.html
- OSPF Area Transit Capability—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_area_trans.html
- PBACL (Policy Based Access Control Lists)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/acl.html#Policy-Based_ACLs
- PBR Support for Multiple Tracking Options—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_pi/configuration/guide/iri_prb_mult_track.html
- Per Interface Netflow—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/netflow.html#Per_Interface_NetFlow
- Periodic MIB Data Collection and Transfer Mechanism—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_mib_collect_trans.html
- Per port VTP enable/disable—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vtp.html#Configuring_VTP_Mode_on_a_Per-Port_Basis
- Persistent Self-Signed Certificates—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pki.html
- Per-VRF Assignment of BGP Router-ID—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_router_id.html
- PIM Triggered Joins—See this publication:

  http://www.cisco.com/en/US/docs/ios/ios_xe/ipmulti/configuration/guide/imc_high_availability_xe.html
- Port-Based Access Control Lists (PACLs)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.html
- Private Hosts—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/pvthost.html

- QoS Support on Bridging Features—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgsip.html#QoS_Traffic_Class_Configuration_Guidelines

- Reliable Static Routing Back-up using Object Tracking—See these publications:

  http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_rel_stc_rtg_bckup.html

  http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/dia_rel_stc_rtg_bckup_ps6441_TSD_Products_Configuration_Guide_Chapter.html

- Reverse Route Injection (RRI)—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_rev_rte_inject.html

- Router Guard—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/igmpfilt.html#Understanding_Router_Guard

- RSVP Message Authentication—See this publication:

  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/rsvp_msg_auth.html

- Scalable EoMPLS (SIP-Based)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgeth.html#Scalable_EoMPLS

- SmartPorts—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/smrtport.html

- SNMP Support over VPN—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/netmgmt/configuration/guide/nm_cfg_snmp_sup_xe.html

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_snmp_sup.html

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_snmp_sup.html#SNMP_Support_for_VPNs

- SPAN Destination Port Support On Etherchannels—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html#Local_SPAN,_RSPAN,_and_ERSPAN_Destinations

- SPAN Egress Session Increase—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html#Local_SPAN,_RSPAN,_and_ERSPAN_Session_Limits

- SSO - GLBP—See these publications:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ha/configuration/xe-3s/ha-config-stateful-switchover.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-glbp.html

- SSO - HSRP—See these publications:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ha/configuration/xe-3s/ha-config-stateful-switchover.html

  http://www.cisco.com/en/US/docs/ios/ios_xe/ipapp/configuration/guide/ipapp_hsrp_xe.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-hsrp.html

- Support for MPLS-VPN Software Modularity—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ios_sw_mod_l3_vpn.html

- Suppress BGP Advertisement for Inactive Routes—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_basic_net.html

- Switch Port Analyzer (SPAN) - CPU Source—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html#Source_CPUs

- Switch Port Analyzer (SPAN) - Distributed Egress SPAN—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html#Monitored_Traffic_Direction

- Switch Port Analyzer (SPAN) - Input Packets with Don't Learn Option—See these publications:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html#Configuring_ERSPAN

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html#Configuring_Local_SPAN

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html#Configuring_RSPAN

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html#Local_SPAN,_RSPAN,_and_ERSPAN_Destinations

  **Note** See the information about the **ingress** keyword.

- TCP MSS Adjust—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/ipapp/configuration/guide/ipapp_tcp_xe.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-2sx/iap-tcp.html

- Two-Rate Policer—See these publications:

  http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/two_rate_policer_xe.html

  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/two_rate_policer.html

- Universal Boot Loader—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/overview.html#Universal_Boot_Loader_Image

- Unknown Unicast Flood Rate-Limiting—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/blocking.html

- VLAN Locking—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vlans.html#VLAN_Locking

- VPLS Multiple VCs per Spoke—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgsip.html#Configuring_Virtual_Private_LAN_Service_

- VRF Aware Multicast Error Messages—The VRF Aware Multicast Error Messages feature improves the troubleshooting of MPLS VPN environments by allowing service providers to track the multicast error messages that are associated with a particular MVPN customer.
- VRF Aware System Message Logging (Syslog)—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vrf_aware_loggng.html
- Web Authentication Proxy—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/webauth.html

# Software Features from Earlier Releases

- 4000 ATM VCs per port adapter on the following FlexWAN ATM port adapters:

  PA-A3-OC3MM

  PA-A3-OC3SMI

  PA-A3-OC3SML

  PA-A3-T3

  PA-A3-E3

  PA-A6-OC3MM

  PA-A6-OC3SMI

  PA-A6-OC3SML

  PA-A6-T3

  PA-A6-E3
- 4096 Layer 2 VLANs—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "VLAN Ranges" section in the "Configuring VLANs" chapter.

  **Note** We recommend that you configure a combined total of no more than 2,000 Layer 3 VLAN interfaces and Layer 3 ports.
- Any Transport over MPLS (AToM) Features:
  - Not supported with PFC3A
  - Supported on WAN ports
  - Ethernet over MPLS (EoMPLS)
  - Frame Relay over MPLS (FRoMPLS)
  - ATM Single Cell Relay over MPLS-VC Mode (CRoMPLS)
  - ATM AAL5 over MPLS (AAL5oMPLS)
  - HDLC over MPLS (HDLCoMPLS)—Note these guidelines and restrictions:

    HDLCoMPLS supports core-facing ports only on Enhanced FlexWAN modules and Shared Port Adapter (SPA) Interface Processors (SIPs).

  - PPP over MPLS (PPPoMPLS)—Note these guidelines and restrictions:

    All PPP negotiations (for example, link control protocol [LCP] negotiations) and keepalives are end to end from CE to CE. The PE routers do not participate in PPP negotiations.

    Multilink PPPoMPLS (MLPPPoMPLS) is not supported, but it can be emulated. To emulate MLPPPoMPLS, each member link of the MLPPP bundle on a CE requires a corresponding PPPoMPLS tunnel on the PE router that it directly connects to. For example, if an MLPPP bundle has three member links, you must configure three PPPoMPLS tunnels on each PE with each tunnel corresponding to a member link.

  See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/12-2sx/mp-any-transport.html

- ATM Cell Loss Priority (CLP) Setting on FlexWAN module ATM interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- ATM OAM ping—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12satmpng.html

- ATM VC access trunk emulation—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html

- ATM Virtual Circuit (VC) Bundling—See these publications:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfipaov.html

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsmu26s.html

- Autostate - Firewall Capability for the Firewall service module—See this publication:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

- Bandwidth Command for HQoS Parent Class Support—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgsip.html#Configuring_Virtual_Private_LAN_Service_(VPLS)

- BGP Configuration Using Peer Templates—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpct.html

- BGP Cost Community—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpcc.html

- BGP Dynamic Update Peer-Groups—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpdpg.html

- BGP Increased Support of Numbered AS-path Access Lists to 500—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.html

- BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/fsxeibmp.html

**Note** With the BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN feature configured, do not attach output service policies to VRF interfaces. (CSCsb25509)

For nonMPLS environments, see the Interior Border Gateway Protocol (iBGP) Multipath Load Sharing feature.

- BGP Policy Accounting—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgppa.html
- BGP Restart Session After Max-Prefix Limit—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html#BGP_Neighbor_Session_Restart_After_the_Max-Prefix_Limit_Is_Reached
- BGP Route Map Continue—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/t_bgprco.html
- BGP Route-Map Policy List Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/t_bgprco.html
- BGP support for TTL security check—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/12-2sx/irg-neighbor.html
- Bidirectional Forwarding Detection (BFD) standard implementation—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  **Note** Catalyst 6500 switches support BFD only on Ethernet, Fast Ethernet (except PA-2FE and PA-1FE), Gigabit Ethernet, and 10-Gigabit Ethernet ports, including Ethernet SPAs. The Catalyst 6500 switches and Cisco 7600 routers do not support BFD on PA-2FE or PA-1FE Ethernet LAN ports, or on POS, ATM, or serial WAN ports.

  Also see “Integrated IS-IS support for BFD over IPv4” and “OSPF support for BFD over IPv4.”
- Bidirectional Protocol Independent Multicast (PIM) in hardware—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Understanding IPv4 Bidirectional PIM” section in the “Configuring IPv4 Multicast Layer 3 Switching” chapter.
- Boot Protocol (BOOTP) relay—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf012.html
- Bridge Control Protocol (BCP)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html
- Bridging using RFC1483 Routed Encapsulation (BRE)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- Certificate Autoenrollment (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html

- Certificate Security Attribute-Based Access Control (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html

- Cisco IOS IP Event Dampening—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/configuration/12-2sx/iri-ip-event-damp.html

- IPv6 Switching: Provider Edge Router over MPLS (6PE) (not supported in PFC3A mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-over-mpls.html

- Cisco IOS Secure Copy (SCP)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-secure-copy.html

- Cisco IOS server load balancing (SLB):
  - GGSN-SLB Messaging
  - Home Agent Loadbalancing

  See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxd1.html

**Note** Web Cache Control Protocol (WCCP) Layer 2 PFC redirection is supported with Cisco IOS server load balancing (SLB). Other WCCP configurations are not compatible with Cisco IOS server load balancing (SLB).

- Cisco IOS server load balancing (SLB): interface-aware—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.html

- Cisco IOS server load balancing (SLB): stateful failover within single chassis—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.html

- Cisco IP Phone Support—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Cisco IP Phone Support" chapter.
- Cisco Nonstop Forwarding (NSF) with stateful switchover (SSO) supervisor engine redundancy—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring NSF with SSO Supervisor Engine Redundancy" chapter.

**Note**

- With PFC3, NSF with SSO supports multicast traffic.
- NSF with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, IPX, or MPLS.
- These protocols can coexist with NSF with SSO redundancy mode, but there is no stateful support for them:
  - MPLS and LDP
  - GLBP
  - HSRP
  - VRRP

Following an NSF with SSO switchover, traffic loss occurs on the links where the protocols are configured until the protocols converge.

- Clear hardware interface counters—See this publication:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

- CNS Interactive CLI—Network management applications can use the Cisco Networking Services (CNS) agents to manage network routers. The CNS agent provides the capability to send commands to a router from a programmable source. The CNS Interactive CLI feature introduces a new XML interface that allows you to send interactive commands to a router, such as commands that generate prompts for user input. A benefit of this feature is that interactive commands can be aborted before they have been fully processed. For example, for commands that generate a significant amount of output, the XML interface can be customized to limit the size of the output or the length of time allowed for the output to accumulate. The capability to use a programmable interface to abort a command before its normal termination (similar to manually aborting a command) can greatly increase the efficiency of diagnostic applications that might use this functionality. The new XML interface also allows for multiple commands to be processed in a single session. The response for each command is packaged together and sent in a single response event.
- Configurable Per VLAN MAC Learning (PVL)—See the **mac-address-table learning** command in this publication:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

- Control Plane DSCP Support for RSVP—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/15-mt/rsvp-dscp-spt-for-rsvp.html

- Crypto Conditional Debug Support (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/12-2sx/sec-crypto-debug-sup.html

- IEEE 802.1Q Custom Ethertype:
  - Supported on these modules:

    —Supervisor engines
    —WS-X6708-10GE
    —WS-X6704-10GE
    —WS-X6748-GE-TX
    —WS-X6748-SFP
    —WS-X6724-SFP
    —WS-X6816-GBIC
    —WS-X6516-GE-TX
    —WS-X6516A-GBIC
    —WS-X6516-GBIC

    **Note** The WS-X6516A-GBIC and WS-X6516-GBIC modules apply a configured custom EtherType field value to all ports supported by each port ASIC (1 through 8 and 9 through 16).

  - In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring a Custom IEEE 802.1Q EtherType Field Value" section in the "Configuring LAN Ports for Layer 2 Switching" chapter.

- Data-link switching plus (DLSw+)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcfdlsw_external_docbase_0900e4b180753b82_4container_external_docbase_0900e4b180771fb6.html

- DE/CLP and EXP mapping on FR/ATMoMPLS VC—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/pfc3mpls.html#DE/CLP_and_EXP_Mapping_on_FR/ATMoMPLS_VC

- DHCP Option 82 on Untrusted Port—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Packet Validation" section in the "Configuring DHCP Snooping" chapter.
- DHCP Snooping—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring DHCP Snooping" chapter.
- Digital Optical Monitoring (DOM)—See the **show interfaces transceiver** command in this publication:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

  **Note** See this publication for additional information about DOM:

  http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_8031.html

- Directed broadcasts with the **mls ip directed-broadcast** command supported in hardware—See this publication:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

- Distinguished Name-Based Crypto Maps (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/12-2sx/sec-dist-nm-cyrpto.html

- Distributed LFI (dLFI) and distributed QoS (dQoS) over Leased Lines on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_latjit/configuration/15-mt/qos-mlppp-fr.html

- Distributed MLPPP (dMLPPP) on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

  **Note** cRTP is not supported on dMLPPP bundled links.

- Distributed Multilink Frame Relay (FRF.16)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/dmfr.html

- Distributed network-based application recognition (dNBAR) on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_4t/qos/configuration/guide/qsnbar1.html

- Dynamic ARP Inspection (DAI)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Dynamic ARP Inspection" chapter.
- Dynamic Host Configuration Protocol (DHCP)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfdhcp.html

- Dynamic Multipoint VPN (DMVPN) Phase 2 (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-s/sec-conn-dmvpn.html

- Easy VPN Server features (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_esyvpn/configuration/12-2sx/sec-easy-vpn-12-2sx-book.html

- EIGRP MPLS VPN PE-CE site of origin (SoO)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_mvesoo.html

- Embedded network management improvements—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

- Encapsulated Remote SPAN (ERSPAN)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Local SPAN, RSPAN, and ERSPAN" chapter.

- Encrypted Multicast over GRE (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- Encrypted Preshared Key (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/12-2sx/sec-encrypt-preshare.html

- EtherChannel—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring EtherChannels" chapter.

- EtherChannel Enhancement - 128 EtherChannels Support—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "EtherChannel Feature Overview" section in the "Configuring EtherChannels" chapter.

- EtherChannel Min-Links—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring the EtherChannel Min-Links Feature" section in the "Configuring EtherChannels" chapter.

- Ethernet over MPLS (EoMPLS) per VLAN QoS—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgeth.html#EoMPLS_Configuration_Example

- Flex Links—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Flex Links" chapter.

- Frame Relay virtual circuit (VC) bundling—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html

- Gateway Load Balancing Protocol (GLBP)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_glbp2.html

- Generic Online Diagnostics (GOLD)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Online Diagnostics" chapter and the "Online Diagnostic Tests" appendix.

- Half-Bridging on FlexWAN ATM interfaces (CSCin27157)

- Hardware Capacity Monitoring—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Determining System Hardware Capacity" section in the "Power Management and Environmental Monitoring" chapter.
- Hardware Control Plane Interface for Control Plane Policing (CoPP):
  - Release 12.2SX does not support CoPP output rate limiting (policing).
  - Release 12.2SX does not support the CoPP silent operation mode.
  - Release 12.2SX does not support the **match protocol arp** command.
  - Release 12.2SX automatically installs the CoPP service policy on all DFC-equipped switching modules.
  - In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Control Plane Policing" chapter.
- Hardware-supported counters for hardware-supported ACLs, displayed by the **show tcam interface** command (not supported in PFC3A mode). See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s6.html#GUID-1D17939B-1C8F-422C-83CE-64B096DAD13D
- HQoS support for Ethernet over MPLS (EoMPLS) VC—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- H-VPLS with MPLS Edge—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgsip.html#Configuring_Virtual_Private_LAN_Service_(VPLS)
- IDSM-2 EtherChannel load balancing—See this publication:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/tsd_products_support_model_home.html
- IEEE 802.1Q protocol tunneling—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Layer 2 Protocol Tunneling" chapter.
- IEEE 802.1Q tunneling—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring IEEE 802.1Q Tunneling" chapter.
- IEEE 802.1s - Multiple Spanning Tree (MST) Standard Compliance—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Understanding MST" section in the "Configuring STP and MST" chapter.
- IEEE 802.1w, rapid reconfiguration of spanning tree; also called Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Understanding IEEE 802.1w RSTP" section in the "Configuring STP and MST" chapter.
- IEEE 802.1X Port-Based Authentication—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring IEEE 802.1X Port-Based Authentication" chapter.
- IEEE 802.3ad, link aggregation control protocol (LACP)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Understanding IEEE 802.3ad LACP EtherChannel Configuration" section in the "Configuring EtherChannels" chapter.
- IGMP snooping and the IGMP snooping querier—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring IGMP Snooping and MVR for IPv4 Multicast Traffic" chapter.

- IGMP Static Group Range Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/stgrpsxf.html

- IKE: Initiate Aggressive Mode (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/12-2sx/sec-aggr-mde-ike.html

- Integrated IS-IS global default metric—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-mt/irs-netd.html

- Integrated IS-IS protocol shutdown support maintaining configuration parameters—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_isis/configuration/guide/irs_initcf.html

- Integrated IS-IS support for BFD over IPv4—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  **Note** Also see Bidirectional Forwarding Detection (BFD) standard implementation.

- Interior Border Gateway Protocol (iBGP) Multipath Load Sharing—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgpls.html

  **Note** For MPLS support, see BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN.

- Internet Group Management Protocol Version 3 (IGMPv3) snooping—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "IGMP Version 3 Support Overview" section in the "Configuring IGMP Snooping and MVR for IPv4 Multicast Traffic" chapter.

- Invalid Special Parameter Index (SPI) Recovery—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dplane/configuration/12-2sx/sec-invald-index-rec.html

- Inverse Multiplexing over ATM (IMA) on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- IP-in-IP tunneling and generic routing encapsulation (GRE) tunneling (hardware-assisted)—The PFC3 and DFC3s support the following tunnel commands:

  - **tunnel destination**
  - **tunnel mode gre**
  - **tunnel mode ipip**
  - **tunnel source**
  - **tunnel ttl**
  - **tunnel tos**

  Other supported types of tunneling run in software on the MSFC3. The PFC3 does not provide hardware acceleration for tunnels configured with the **tunnel key** command.

  The **tunnel ttl** command (default 255) sets the TTL of encapsulated packets.

The **tunnel tos** command, if present, sets the ToS byte of a packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is not enabled, the ToS byte of a packet sets the ToS byte of the packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is enabled, the ToS byte of a packet as modified by PFC QoS sets the ToS byte of the packet when it is encapsulated.

To configure GRE Tunneling and IP in IP Tunneling, refer to these publications:

http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html

http://www.cisco.com/en/US/docs/ios/12_2/interface/command/reference/irfshoip.html

To configure the **tunnel tos** and **tunnel ttl** commands, refer to this publication:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html

Note the following information about tunnels:

- Each hardware-assisted tunnel must have a unique source address. Hardware-assisted tunnels cannot share a source address even if the destination addresses are different. Use secondary addresses on loopback interfaces or create multiple loopback interfaces. Failure to use unique source addresses may result in control plane failures when software path congestion occurs. (CSCdy72539)
- Each tunnel interface uses one internal VLAN.
- Each tunnel interface uses one additional router MAC address entry per router MAC address.
- The PFC3A does not support any PFC QoS features on tunnel interfaces.
- The PFC3B and PFC3BXL support PFC QoS features on tunnel interfaces.
- In releases earlier than Release 12.2(18)SXE, the PFC3 does not support GRE tunnel encapsulation and de-encapsulation of multicast traffic.
- The MSFC supports tunnels configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT and PAT (for inside to outside translation), TCP intercept, and encryption.

- IP routing of RFC1483 ATM bridge encapsulation (RBE)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html

- IPSec Anti-Replay Window: Expanding and Disabling—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dplane/configuration/12-2sx/sec-ipsec-antireplay.html

- IP Security VPN Monitoring (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_imgmt/configuration/12-2sx/sec-ip-security-vpn.html

- IPsec VPN Accounting (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_imgmt/configuration/12-2sx/sec-ipsec-vpn-actg.html

- IPS Inline VLAN Pairing for WS-SVC-IDSM2-K9—See this publication for more information:

  http://www.cisco.com/en/US/docs/security/ips/5.1/configuration/guide/cli/cliguide.html

- IP Unnumbered for VLAN-SVI interfaces—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Subinterfaces on Layer 3 Interfaces" section in the "Configuring Layer 3 Interfaces" chapter.

- IPv6 access services: DHCPv6 prefix delegation—See this publication: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/15-sy/ipv6-15-sy-library.html
- IPv6—Hardware support for these basic IPv6 functions:
  - IPv6 standard access control lists (ACLs)
  - IPv6 extended ACLs
  - Reflexive ACLs
  - Manually configured v6 tunnels
  - ISATAP (ISATAP with 6-to-4 prefix is not supported in hardware)
  - Automatically configured IPv4 compatible tunnels
  - 6-to-4 tunnel
  - IPv6 over IPV4 IP in IP tunnels
- IPv6—Software support for these basic IPv6 functions:
  - IPv6 addressing architecture
  - ICMPv6
  - Neighbor Discovery
  - Static ND cache entry
  - IPv6 stateless autoconfiguration
  - ICMPv6 Redirect
  - MTU path Discovery for IPv6
  - IPv6 ICMP rate limiting
  - IPv6 over IPV4 GRE tunnels
- IPv6—Software support for IPv6 routing:
  - Static routes within IPv6
  - RIPng
  - MP-BGP4
  - OSPFv3
  - ISIS
  - Configuring an IPv6 Multiprotocol BGP Peer using a link local address
  - IPv6 MP-BGP distance command
- IPv6—Switching support for IPv6:
  - Process
  - CEFv6
  - Distributed CEFv6
- IPv6—Software support for these IPv6 applications:
  - Ping
  - Traceroute
  - Telnet
  - TFTP (client only)

  - FTP
  - SSH over IPv6
  - DNS
  - HTTP server

  For configuration information, refer to this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/15-sy/ipv6-15-sy-library.html

  For command reference information, refer to this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

- IPv6 hardware: multicast assist—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring IPv6 Multicast PFC3 and DFC3 Layer 3 Switching" chapter.
- IPv6 multicast: Bootstrap Router (BSR)—See the BSR information in the *Cisco IOS IPv6 Configuration Library* and the *Cisco IOS IPv6 Command Reference*.
- IPv6 Multicast: HW assisted egress replication—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Displaying the Replication Mode Auto Detection Status" section in the "Configuring IPv6 Multicast PFC3 and DFC3 Layer 3 Switching" chapter.
- IPv6 multicast RPR support—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring RPR Supervisor Engine Redundancy" chapter.
- IPv6 QoS: (quality of service)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "General Guidelines" section in the "Configuring PFC QoS" chapter.
- IPv6 Support on WAN Interfaces—See this publication:

  http://www.cisco.com/en/US/tech/tk872/tech_white_papers_list.html
- IS-IS caching of redistributed routes—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isredrib.html
- IS-IS Incremental SPF—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isisispf.html
- IS-IS Limit on Number of Redistributed Routes—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsiredis.html
- IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsisiadv.html
- IS-IS support for priority-driven IP prefix RIB installation—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslocrib.html
- IS-IS Support for Route Tags—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-mt/irs-isis-supp-route-tags.html

- Jumbo frames on all Ethernet ports except ports on the WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6148-GE-TX, and WS-X6148V-GE-TX switching modules.

**Caution** The following switching modules support a maximum ingress frame size of 8092 bytes:

- WS-X6516-GE-TX when operating at 100 Mbps
- WS-X6148-RJ-45, WS-X6148-RJ-45V and WS-X6148-RJ21, WS-X6148-RJ21V
- WS-X6248A-RJ-45
- WS-X6348-RJ-45, WS-X6348-RJ45V and WS-X6348-RJ21V

When jumbo frame support is configured, these modules drop ingress frames larger than 8092 bytes.

- Key rollover for certificate renewal—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html

- L3 MPLS VPN over GRE on 7600-SIP-400—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- Layer 2 switch ports and VLAN trunks with the Dynamic Trunking Protocol (DTP), including support on Gigabit Ethernet ports for jumbo frames—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring LAN Ports for Layer 2 Switching" chapter.
- Layer 2 traceroute—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Using the Layer 2 Traceroute Utility" chapter.
- Link Fragmentation and Interleaving (LFI) for FlexWAN Frame Relay interfaces and ATM Virtual Circuits—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_latjit/configuration/15-mt/qos-mlppp-fr.html

- The ip local-proxy-arp command.

  **Note** To use the local proxy ARP feature, you must enable the IP proxy ARP feature. The IP proxy ARP feature is enabled by default. See the ip proxy-arp command documentation.

- Low Latency Queueing (LLQ) and Class-based Weighted Fair Queueing (CBWFQ) on FlexWAN MLPPP links—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html

- MAC address-based traffic blocking—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring MAC Address-Based Traffic Blocking" section in the "Configuring Network Security" chapter.
- Manual Certificate Enrollment (supported with SPA-IPSEC-2G):
  - Also called TFTP and Cut-and-Paste
  - See this publication:

    http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html

- Mapping a subinterface to an EoMPLS VC on 7600-SIP-400—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- match cos classification on 7600-SIP-400—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- MLD snooping—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring MLD Snooping for IPv6 Multicast Traffic" chapter.

- MPLS Basic, including Provider (P) and Provider Edge (PE) functionality (MPLS; not supported in PFC3A mode)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/pfc3mpls.html#Basic_MPLS_Load_Balancing

- MPLS Label Distribution Protocol (LDP; not supported in PFC3A mode)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#MPLS_Support_on_OSMs

- MPLS LDP - Inbound Label Binding Filtering—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsinbd4.html

- MPLS LSP ping/traceroute and AToM VCCV—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_lspng.html

- MPLS Traffic Engineering DiffServ Aware (DS-TE)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsdserv3.html

  **Note** Also see MPLS Traffic Engineering (TE) Fast Reroute (FRR) Link and Node Protection.
  MPLS DS-TE is not supported on these interface types:
  —Port channel interfaces
  —Switch virtual interfaces (SVIs)
  —Multiple link point-to-point protocol (MLPPP) interfaces
  —Multilink Frame Relay (MLFR or MFR)

- MPLS Traffic Engineering Forwarding Adjacency—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fstefa_3.html

- MPLS Traffic Engineering (TE) Fast Reroute (FRR) Link and Node Protection—See these publications:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsfrr24.html

  **Note** Also see MPLS Traffic Engineering DiffServ Aware (DS-TE).
  MPLS TE FRR Link and Node Protection is not supported on these interface types:
  —Port channel interfaces
  —Switch virtual interfaces (SVIs)
  —Multiple link point-to-point protocol (MLPPP) interfaces
  —Multilink Frame Relay (MLFR or MFR)

- MPLS Traffic Engineering (TE) Interarea Tunnels—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiarea3.html

- MPLS Virtual Private Networks (MPLS VPN; not supported in PFC3A mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsmvpns.html

- MPLS VPN Carrier Supporting Carrier (not supported in PFC3A mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs2scsc.html

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fscsclbl.html

- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution (not supported in PFC3A mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiaslbl.html

- MPLS VPN—OSPF and Sham-Link Support (not supported in PFC3A mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_sham_link.html

- MPLS VPN ID (not supported in PFC3A mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/vpnid2.html

- MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) —See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/12-2sx/ire-mpls-vpn.html

  **Note** The MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) feature also provides EIGRP support for VRF Lite.

- MQC: distribution of remaining bandwidth (supported only on WAN ports)—You configure QoS features on an interface using the modular QoS CLI (MQC). Using MQC, you create service policies for traffic classes and attach the policies to an interface. You can use MQC to specify how the remaining bandwidth is distributed among the interface or subinterface output queues. The remaining bandwidth is the available bandwidth left on an interface or subinterface after all guaranteed traffic is accounted for. The amount of remaining bandwidth available for use is determined by the excess information rate (EIR) configured for the queue.

  The **bandwidth remaining percent** command allows you to configure the remaining bandwidth for output queues. The aggregate of all user-configured EIR bandwidth percentages cannot exceed 100 percent. If the aggregate of all remaining bandwidth is less than 100 percent, the remainder is evenly split among user queues (including the default queue) that do not have a remaining bandwidth percentage configured. The minimum EIR value of each output queue is 1.

  This example shows how to use the **bandwidth remaining percent** command to distribute percentages of remaining bandwidth to various traffic classes in a policy map:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map myPolicy
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20
Router(config-pmap-c)# class prec1
Router(config-pmap-c)# bandwidth remaining percent 30
Router(config-pmap-c)# class prec2
Router(config-pmap-c)# bandwidth remaining percent 10
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
```

```
Router# show policy-map myPolicy
  Policy Map myPolicy
    Class prec1
         bandwidth remaining percent 30
    Class prec2
         bandwidth percent 50
         bandwidth remaining percent 10
    Class class-default
         bandwidth remaining percent 20
Router#
```

- Multicast enhancement - egress replication performance improvement and Multicast Enhancement - Replication Mode Detection—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring the Replication Mode" and "Enabling Local Egress Replication" sections in the "Configuring IPv4 Multicast Layer 3 Switching" chapter.
- Multicast-VPN: Multicast Support for MPLS VPN—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring IPv4 Multicast VPN Support" chapter.

**Note** Support for MVPN also includes support for multicast VRF (MVRF). MVRF is also known as multicast over VRF-lite. MVPN and MVRF are supported in PFC3B or PFC3BXL mode and PFC3C or PFC3CXL mode.

- Multiple-Hot Standby Routing Protocol (MHSRP)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfip.html
- Multiple RSA Key Pair Support (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-deploy-rsa-pki.html
- Multipoint bridging (MPB)—See these publications:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html
- NAC - L2 IP; Network Admission Control (NAC) Layer 2 Layer 2 IP validation—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Network Admission Control" chapter.
- NetFlow Aggregation (hardware assisted)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring NetFlow Aggregation" section in the "Configuring NetFlow" chapter.
- NetFlow - Bridged Flow Statistics—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Enabling NetFlow for Ingress-Bridged IP Traffic" section in the "Configuring NetFlow" chapter.
- NetFlow Data Export (NDE)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring NDE" chapter.

- NetFlow multicast support:
  - Supported only with NetFlow v9 export format.
  - See this publication:

    http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/12-2sx/cfg-nf-multi-acctg.html
  - The NetFlow Multicast Support document contains a prerequisite that does not apply when configuring NetFlow multicast support with Release 12.2(18)SXF and later 12.2SX releases:

    You do not need to configure multicast fast switching or multicast distributed fast switching (MDFS); multicast CEF switching is supported with Release 12.2(18)SXF and later 12.2SX releases.
- NetFlow Multiple Export Destinations:
  - Allows entry of a second **ip flow-export destination** command
  - See In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring the NDE Destination" section in the "Configuring NDE" chapter.
- NetFlow v9 Export Format, including NetFlow Export of BGP Nexthop Information—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/12-2sx/cfg-nflow-data-expt.html
- Network Address Translation (NAT) and Port Address Translation (PAT) for IPv4 unicast and multicast traffic (hardware assisted)—Note the following information about hardware-assisted NAT:
  - The PFC3A does not support NAT or PAT for UDP traffic.

    **Note** PFC3B and PFC3BXL modes support NAT and PAT for UDP traffic.
  - The PFC3 does not support NAT or PAT for multicast traffic.
  - The PFC3 does not support NAT or PAT configured with a route map that specifies length.
  - The PFC3 does not support NAT or PAT configured with a route map that specifies static translations.
  - When you configure NAT or PAT and NDE on an interface, the PFC3 sends all traffic in fragmented packets to the MSFC3 to be processed in software. (CSCdz51590)

  To configure NAT or PAT, refer to the Cisco IOS IP Configuration Guide, Release 12.2, "IP Addressing and Services," "Configuring IP Addressing," "Configuring Network Address Translation," at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfipadr.html

  For information about configuring NAT or PAT with route maps, refer to this publication:

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_q_and_a_item09186a00800e523b.shtml

  To prevent a significant volume of NAT or PAT traffic from being sent to the MSFC, due to either a DoS attack or a misconfiguration, enter the **mls rate-limit unicast acl** {**ingress** | **egress**} command described in this publication:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

  (CSCea23296)

- Optimized ACL logging (supported only with PFC3)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Optimized ACL Logging" section in the "Understanding Cisco IOS ACL Support" chapter.
- OSPF Forwarding Address Suppression in Translated Type-5 LSAs—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/12-2sx/iro-for-add-sup.html
- OSPF Inbound Filtering Using Route Maps with a Distribute List—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/routmap.html
- OSPF Incremental Shortest Path First (i-SPF)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfispf.html
- OSPF Limit on Number of Redistributed Routes—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsoredis.html
- OSPF link-local signaling (LLS) per interface basis—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospflls.html
- OSPF link state database overload protection—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfopro.html
- OSPF MIB support of RFC 1850 and latest extensions—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html
- OSPF Shortest Path First Throttling—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_spftrl.html
- OSPF support for BFD over IPv4—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  **Note** Also see "Bidirectional Forwarding Detection (BFD) standard implementation."
- OSPF Support for Fast Hellos—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fasthelo.html
- OSPF support for forwarding adjacencies over MPLS traffic engineered tunnels—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospffa.html
- OSPF Support for Link State Advertisement (LSA) Throttling—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsolsath.html
- OSPF support for unlimited software VRFs per provider edge (PE) router—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/12-2sx/iro-un-sw-vrfs.html
- Packet classification based on layer3 packet-length (supported on WAN ports)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_classn/configuration/12-2sx/qos-classn-ntwk-trfc.html

- Per Interface Sticky ARP—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Sticky ARP" section in the "Configuring Denial of Service Protection" chapter.
- Per port MAC limiting—See the **mac-address-table limit** command in this publication:

  http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
- PFC3 hardware support for IPv4 multicast over point-to-point GRE tunnels—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html

  **Note** Releases earlier than Release 12.2(18)SXE supported IPv4 multicast over point-to-point GRE tunnels in software on the MSFC. The PFC3 does not provide hardware acceleration for tunnels configured with the **tunnel key** command.

- PFC QoS—PFC-hardware assisted Quality of Service (QoS)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring PFC QoS" chapter.
- PFC QoS ARP ACLs for QoS Filtering—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring ARP ACLs for QoS Filtering" section in the "Configuring PFC QoS" chapter.
- PFC QoS DSCP-based Queue Mapping (supported on WS-X6708-10GE and CAT6000-VS-S720-10G/MSFC3)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring DSCP-Based Queue Mapping" section in the "Configuring PFC QoS" chapter.
- PFC QoS DSCP transparency (also called Received ToS byte preservation)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring DSCP Transparency" section in the "Configuring PFC QoS" chapter.
- PFC QoS egress ACL support for remarked DSCP—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Enabling Egress ACL Support for Remarked DSCP" section in the "Configuring PFC QoS" chapter.
- PFC QoS egress DSCP mutation—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Egress DSCP Mutation" section in the "Configuring PFC QoS" chapter.
- PFC QoS egress policing for LAN ports configured as Layer 3 interfaces and for VLAN interfaces—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Attaching a Policy Map to an Interface" section in the "Configuring PFC QoS" chapter.
- PFC QoS features on tunnels (not supported in PFC3A mode)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "PFC QoS Configuration Guidelines and Restrictions" section in the "Configuring PFC QoS" chapter.
- PFC QoS filtering in MAC ACLs per-VLAN and CoS-based (not supported in PFC3A mode)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring MAC ACLs" section in the "Configuring PFC QoS" chapter.
- PFC QoS - Ignore Port Trust—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Enabling Ignore Port Trust" section in the "Configuring PFC QoS" chapter.
- PFC QoS Ingress CoS mutation on IEEE 802.1Q tunnel ports—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Ingress CoS Mutation on IEEE 802.1Q Tunnel Ports" section in the "Configuring PFC QoS" chapter.

- PFC QoS Protocol-Independent MAC ACL Filtering (not supported in PFC3A mode)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Protocol-Independent MAC ACL Filtering" section in the "Configuring PFC QoS" chapter.
- PFC QoS SRR (Shaped Round Robin)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Allocating Bandwidth Between Standard Transmit Queues" section in the "Configuring PFC QoS" chapter.
- PFC QoS user-based microflow policing—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Microflow Policers" section in the "Configuring PFC QoS" chapter for information about configuring microflow policing based on either source or destination addresses.
- PIM Snooping—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring PIM Snooping" chapter.
- PIM snooping DR flooding enhancement—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Disabling PIM Snooping Designated-Router Flooding" section in the "Configuring PIM Snooping" chapter.
- PKI AAA authorization using the entire subject name—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html
- Policy-based routing (PBR) with hardware assist for route-map sequences that use the **match ip address**, **set ip next-hop**, and **set ip default next-hop** PBR keywords.

  To configure PBR, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, "Classification," "Configuring Policy-Based Routing," at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpbr.html

  When configuring PBR, follow these guidelines and restrictions:

  - Releases earlier than Release 12.2(33)SXH use the syntax from Release 12.1, which supports **preempt** as a keyword for the **standby priority** command. Release 12.2(33)SXH and later releases use the Release 12.2 syntax, which requires **standby preempt** and **standby priority** to be entered as separate commands:

    http://www.cisco.com/en/US/docs/ios/ipapp/command/reference/iap_s5.html#standby_priority

    http://www.cisco.com/en/US/docs/ios/ipapp/command/reference/iap_s5.html#standby_preempt
  - The PFC provides hardware support for PBR configured on a tunnel interface.
  - The PFC does not provides hardware support for PBR configured with the **set ip next-hop** keywords if the next hop is a tunnel interface.
  - If the MSFC address falls within the range of a PBR ACL, traffic addressed to the MSFC is policy routed in hardware instead of being forwarded to the MSFC. To prevent policy routing of traffic addressed to the MSFC, configure PBR ACLs to deny traffic addressed to the MSFC. (CSCse86399)
  - Any options in Cisco IOS ACLs that provide filtering in a PBR route map that would cause flows to be sent to the MSFC3 to be switched in software are ignored. For example, logging is not supported in ACEs in Cisco IOS ACLs that provide filtering in PBR route maps.
  - PBR traffic through switching module ports where PBR is configured is routed in software if the switching module resets. (CSCee92191)

- Port Security, including Port security on 802.1Q tunnel ports, port security on private VLAN ports, port security on trunk ports, port security with 4096 secure MAC addresses, and port security with sticky MAC addresses—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Port Security" chapter.
- Private VLANs—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Private VLANs" chapter.
- Protected private key storage—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-deploy-rsa-pki.html
- QoS: Aggregated DSCP / Precedence Values for WRED (supported on for 7600-SIP-400 ATM SPAs)—Aggregates multiple DSCP or IP Precedence values for a single minimum or maximum threshold and marks probability when specifying WRED parameters for 7600-SIP-400 ATM SPAs.
- QoS: ingress shaping on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- QoS Data Export—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring PFC QoS Statistics Data Export" chapter.
- QoS: percentage based policing on WAN ports—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12spctpg.html
- Query mode definition per trustpoint—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html
- Query multiple servers during certificate revocation check—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html
- RADIUS Load Balancing (RLB) IMSI sticky—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.html
- Real-Time Resolution for IPsec Tunnel Peer (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-2sx/sec-realtime-ipsec.html
- Re-enroll using existing certificate—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html
- Remote SPAN (RSPAN)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Local SPAN, RSPAN, and ERSPAN" chapter.
- RFC-1483 Bridging on FlexWAN—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/atm.html
- RFC 1483 Spanning-Tree Interoperability Enhancements on WAN ports—See these publications:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html
- RFC-1490 bridging on FlexWAN interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html

- RFC 1889 Compressed Real-Time Protocol (cRTP) on FlexWAN interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcrtp.html

  **Note** cRTP is not supported on MLPPP bundled links.

- Route Processor Redundancy (RPR)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring RPR Supervisor Engine Redundancy" chapter.
- Router-Port Group Management Protocol (RGMP)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfrgmp.html
- RSVP Interface-based Receiver Proxy—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/rsvpprox.html
- RSVP Refresh Reduction and Reliable Messaging—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsrelmsg.html
- RSVP Scalability Enhancements—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/12-2sx/rsvp-scalability.html
- RSVP Scalability Enhancements—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/12-2sx/rsvp-scalability.html
- SafeNet IPsec VPN client support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/12-2sx/sec-safenet-suppt.html
- SCP health monitoring for enhanced-FlexWAN—The SCP health monitor feature provides improved debugging capabilities for problems that cause WAN module resets because of SCP keepalive failures.
- Secure Shell SSH Version 2 Client Support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-secure-shell-v2.html
- Secure Shell (SSH) Version 2 server support in k9 images—By default, the k9 images support both SSHv1 connections and SSHv2 connections. To restrict connections to either SSHv1 or SSHv2, enter the **ip ssh mode** [**v1** | **v2**] global configuration mode command. Except for the **v1** and **v2** keywords for the **ip ssh mode** command, you configure SSHv2 in the same way as SSHv1. See this publication for more information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-usr-ssh-12-2sx-book.html

  For information about SSHv1 client support, refer to the following publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-usr-ssh-12-2sx-book.html
- Show diagnostic sanity—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Diagnostic Sanity Check" section in the "Configuring Online Diagnostics" chapter.
- Show Top-N—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Using Top-N Reports" chapter.

- SNMP ifindex persistence—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring SNMP IfIndex Persistence" chapter.
- Source Interface Selection for Outgoing Traffic with Certificate Authority (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-sis-with-ca.html
- Source Specific Multicast (SSM) Mapping:
  - Do not configure SSM mapping in a VLAN that supports IGMPv3 multicast receivers.
  - See this publication:

    http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_basic_cfg.html#SSM_Overview
- Source-Specific Multicast with IGMPv3, IGMP v3lite, and URL Rendezvous Directory (URD)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfssm.html
- SPAN—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Local SPAN, RSPAN, and ERSPAN" chapter.
- SPAN destination port permit list—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Destination Port Permit Lists (Optional)" section in the "Configuring Local SPAN, RSPAN, and ERSPAN" chapter.
- Spanning tree PortFast BPDU filtering, PortFast, UplinkFast, and BackboneFast, and Root Guard Feature—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Optional STP Features" chapter.
- Spanning Tree Protocol (STP)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring STP and MST" chapter.
- SSM mapping for IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/15-sy/ipv6-15-sy-library.html
- Standard Domain Naming System (DNS) support—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfipadr.html
- Strict priority low latency queueing (LLQ) on WAN ports—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Configuring_Strict_Priority_Low_Latency_Queuing_(LLQ)_Support_on_the_OSM-2+4GE-WAN+

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pos.html#Configuring_Strict_Priority_LLQ_Support_on_POS_Optical_Service_Modules
- TCP intercept (hardware-assisted)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring TCP Intercept" section in the "Configuring Network Security" chapter.
- TDR cable diagnostics—TDR is supported on these switching modules:
  - WS-X6148-GE-TX
  - WS-X6148V-GE-TX
  - WS-X6148-GE-45AF
  - WS-X6548-GE-TX
  - WS-X6548V-GE-TX
  - WS-X6548-GE-45AF

  - WS-X6748-GE-TX
  - WS-X6148A-GE-TX
  - WS-X6148A-GE-45AF
  - WS-X6148A-RJ-45
  - WS-X6148A-45AF

**Note** TDR can test cables up to a maximum length of 115 meters.

See these publications:

  - In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Checking the Cable Status Using the TDR" section in the "Configuring Interfaces" chapter.
  - The **test cable-diagnostics** command in the command reference at this URL:

    http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html

- Traffic storm control—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Traffic Storm Control" chapter.
- Trusted Root Certification Authority (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_cert_auth_io_OBS.html
- Trustpoint CLI (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html
- UDI - Unique Device Identifier—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/12-2sx/Unique_Device_Identifier_Retrieval.html
- Unicast flood blocking (UFB)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Unknown Unicast Flood Control" chapter.
- Unicast Reverse Path Forwarding (Unicast RPF), hardware-assisted, multiple-path—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Unicast Reverse Path Forwarding Check" section in the "Configuring Network Security" chapter.
- UniDirectional Link Detection—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring UDLD" chapter.
- Uni-Directional Link Routing (UDLR)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring UDE and UDLR" chapter.
- VLAN Access Control Lists (VACLs)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring Port ACLs and VLAN ACLs" chapter.
- VACL capture—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring a Capture Port" section in the "Configuring Port ACLs and VLAN ACLs" chapter.

**Note** VACL capture is not supported on WS-X6708-10GE ports.

- VACL Deny Logging—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring VACL Logging" section in the "Configuring Port ACLs and VLAN ACLs" chapter.
- Virtual Router Redundancy Protocol (VRRP)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-vrrp.html
- VLANs—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring VLANs" chapter.
- VLANs over IP unnumbered sub-interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-i4.html#GUID-833D9D25-1E04-4430-84D8-1AA836DE4745
- VLAN translation—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring VLAN Translation" section in the "Configuring VLANs" chapter.
- VLAN Trunk Protocol (VTP) and VTP domains—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the "Configuring VTP" chapter.
- Voice over Frame Relay (VoFR) FRF.11 and FRF.12 for FlexWAN interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/vvfvofr.html

  **Note** Because Release 12.2SX does not support voice modules, switches supported in Release 12.2SX can act only as a VoFR tandem switch when FRF.11 or FRF.12 is configured on the FlexWAN module.

- VRF Aware IPsec (supported with SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_vrf_aware_ipsec.html
- VRF Lite (Multi-VRF for CE Routers) with IPv4 forwarding between VRFs interfaces, IPv4 ACLs, and IPv4 HSRP (supported on LAN and WAN ports)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_MPLS

  **Note** Multi-VRF for CE Routers (VRF Lite) with the PFC3 supports multi-VRF CE functionality with EIGRP, OSPF, BGP and RIPv2 routing protocols running on a per VRF basis. Static routes are also supported.

- Web Cache Control Protocol (WCCP)—These WCCP features are supported:
  - WCCP L2 Return
  - WCCP Layer 2 PFC Redirection
  - WCCP Redirection on Inbound Interfaces
  - WCCP Version 1
  - WCCP Version 2
  - See this publication:

    http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-2sx/iap-wccp.html

**Note** Release 12.2SX does not support these WCCP features:
—WCCP Layer 2 Redirection/Forwarding
—WCCP Mask Assignment
—WCCP VRF Support

# Unsupported Features and Commands

**Note** See also the "Supervisor Engine 32 Restrictions" section on page 22 and the "Cisco IOS Software Modularity Unsupported Features" section on page 8.

- Hardware—See the "Unsupported Hardware" section on page 112.
- In Release 12.2(33)SXH and later releases:
  - DECNet
  - Route Processor Redundancy Plus (RPR+)
  - Network-based application recognition (NBAR) for LAN interfaces (supported in earlier releases only with Supervisor Engine 2)
- These QoS interface commands are not supported on SPA interfaces:
  - **traffic shape**
  - **priority-group**
  - **custom-queue-list**
  - **tx-queue-limit**
  - **fair-queue**
  - **random-detect**
  - **rate-limit**
  - **tx-ring-limit**
  - **max-reserved-bandwidth**
- These QoS interface commands are not supported on FlexWAN interfaces:
  - **traffic shape**
  - **priority-group**
  - **custom-queue-list**
  - **tx-queue-limit**
- Dot1q Transparency for EoMPLS (supported on OSM ports)
- Metro Ethernet Advanced QinQ Service Mapping (supported on OSM ports)
- Per VLAN load balancing for advanced QinQ service mapping (supported on OSM ports)
- Control Plane DSCP Support for RSVP
- RSVP Scalability Enhancements

- Random Sampled NetFlow (**flow-sampler** commands)
- In releases earlier than Release 12.2(33)SXH, generic routing encapsulation (GRE) tunnel IP source and destination VRF membership (the **tunnel vrf** command). (CSCee39138)
- Warm Reload (CSCef06158)
- ARP Optimization (CSCef30539)
- Exterior Border Gateway Protocol (eBGP) multihop over CSC-PE interfaces (CSCea83165)
- Commands to globally disable EtherChannel or trunking
- **write tech-support** command
- Disable port startup option
- Clear counters per port or clear QoS statistics
- System warning and error counter enhancements implemented in Catalyst software release 6.1(1)
- Command to display the port MAC address
- System warnings on port counters
- VLAN Management Policy Server (VMPS) client or server
- Cisco IOS MAC-layer access control lists (ACLs)
- Cisco IOS firewall feature set (includes context-based access control; CBAC)
- Accelerated server load balancing (ASLB)
- Hot Standby Router Protocol (HSRP) between redundant supervisor engines (the redundant supervisor engine and MSFC are in standby mode—HSRP to external routers is supported)
- Multi-Instance Spanning Tree Protocol (MISTP); IEEE 802.1s MST is supported
- Common Open Policy Server (COPS)
- Except to support tunnels, Resource ReSerVation Protocol (RSVP)
- GARP VLAN Registration Protocol (GVRP)
- GARP Multicast Registration Protocol (GMRP)
- Commands present in the CLI, but not supported:
  - ipv6 cef accounting
  - ip cef accounting
  - module provision

# Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections:


- Cisco IOS Release 12.2(33)SXJ6, page 191
- Cisco IOS Release 12.2(33)SXJ5, page 192
- Cisco IOS Release 12.2(33)SXJ4, page 192
- Cisco IOS Release 12.2(33)SXJ3, page 193
- Cisco IOS Release 12.2(33)SXI12, page 194
- Cisco IOS Release 12.2(33)SXI11, page 194
- Cisco IOS Release 12.2(33)SXI10, page 194
- Cisco IOS Release 12.2(33)SXI9, page 194
- Cisco IOS Release 12.2(33)SXI8a, page 195
- Cisco IOS Release 12.2(33)SXI8, page 195
- Cisco IOS Release 12.2(33)SXI7, page 195
- Cisco IOS Release 12.2(33)SXI6, page 197
- Cisco IOS Release 12.2(33)SXI5, page 197
- Cisco IOS Release 12.2(33)SXH8b, page 198
- Cisco IOS Release 12.2(33)SXH8a, page 199
- Cisco IOS Release 12.2(33)SXH8, page 199
- Cisco IOS Release 12.2(33)SXH7, page 200
- Cisco IOS Release 12.2(33)SXH6, page 201
- Cisco IOS Release 12.2(33)SXH5, page 203


## Cisco IOS Release 12.2(33)SXJ6

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXJ6:

- Route Processor software for NetFlow

  **Old Behavior:** Route Processor (RP) export values (byte/packet counts per flow) are independent of the configured platform NetFlow sampling ratio.

  **New Behavior:** The RP software divides the exported packet/byte counts for V5 and V9 export by the configured platform sampling ratio. To enable this behavior, use the platform netflow rp sampling scale command.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_02.html#platform_netflow_rp_sampling_scale

- New CLI: **mls ipv6 acl pbr svi hardware**

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-i5.html

# Cisco IOS Release 12.2(33)SXJ5

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXJ5:

- Minimum value raised for **port-channel min-links**

  **Old Behavior:** The minimum value for the **port-channel min-links** command was 1.

  **New Behavior:** The minimum value for the **port-channel min-links** command is 2.

- WS-X6066-SLB-APC CSM, WS-X6066-SLB-S-K9 CSM-S, WS-SVC-SSL-1 SSL service module support

  **Old Behavior:** Release 12.2(33)SXJ and rebuilds do not support these services modules, but they power up in the chassis:

  - WS-X6066-SLB-APC  Content Switching Module (CSM)
  - WS-X6066-SLB-S-K9  Content Switching Module with SSL (CSM-S)
  - WS-SVC-SSL-1  Secure Sockets Layer (SSL) Services Module

  **New Behavior:** With Release 12.2(33)SXJ5 and later releases, the modules do not power up in the chassis.

- WiSM QoS untrusted mode

  Old Behavior: By default, WiSM portchannel interface ports are configured toS trust CoS. Other QoS trust modes can be configured, but there is no option to set the mode to "untrusted".

  New Behavior: There is an option to configure the untrusted mode:

```
Router(config)# wism module 4 con 1 qos trust ?
  cos            Trust CoS
  dscp           Trust DSCP
  ip-precedence  Trust IP precedence
  none           UnTrust
```

# Cisco IOS Release 12.2(33)SXJ4

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXJ4:

- Command accounting and command authorization to be sent in asplain notation

  **Old Behavior:** Command accounting and command authorization that include a 4-byte ASN number are sent in the same format that is used on the command-line interface.

  **New Behavior:** Command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

  **Additional information:**

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp3.html

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp4.html

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_10.html

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_11.html

- Fast Network Time Protocol (NTP) synchronization

  **Old Behavior:** The burst and initial burst (iburst) modes are enabled manually.

  **New Behavior:** The burst and iburst modes are enabled by default.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-CC69EFC5-68A3-4C5D-90CD-67DE45D4A370

# Cisco IOS Release 12.2(33)SXJ3

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXJ3:

- Output changes for the **show ip igmp interface vlan** command

  **Old Behavior:** The "IGMP snooping query interval" line from the **show ip igmp interface vlan** command displays the IGMP snooping query interval configured on the switch where you enter the CLI.

  Any redundant IGMP snooping queriers do not use the query interval of the active IGMP snooping querier and instead use the locally configured query interval (or the default). You cannot display the active interval On a switch where a redundant IGMP snooping querier is configured.

  **New Behavior:** The `IGMP snooping query interval` line from the **show ip igmp interface vlan** command displays the IGMP snooping query interval learned from the active IGMP snooping querier or the IGMP Query Interval learned from the active IGMP querier if the IGMP querier is operating in IGMP v3 mode. The **show ip igmp interface vlan** command displays the IGMP snooping query interval configured on the switch where you enter the CLI.

  The `IGMP configured snooping query interval` line from the **show ip igmp interface vlan** command displays the IGMP snooping query interval configured on the switch where you enter the CLI.

  Any redundant IGMP Snooping Queriers learn the active IGMP snooping querier interval. If a redundant IGMP snooping querier becomes active, the newly elected active IGMP snooping querier uses the locally configured IGMP snooping query interval (or the default).

- Default 8q4t DSCP-based queue mapping change

  **Old behavior:**

  queue 1, threshold 1: 0-9, 11, 13, 15-17, 19, 21, 23, 25, 27, 29, 31, 33, 39, 41-45, 47

  queue 2, threshold 1: 14

  queue 2, threshold 2: 12

  queue 2, threshold 3: 10

  queue 3, threshold 1: 22

  queue 3, threshold 2: 20

  queue 3, threshold 3: 18

  queue 4, threshold 1: 24, 30

  queue 4, threshold 2: 28

  queue 4, threshold 3: 26

  queue 5, threshold 1: 32, 34-38

  queue 6, threshold 1: 48-63

queue 8, threshold 1: 40, 46

**New behavior:**

queue 1, threshold 1: 0-9, 11, 13-17, 19, 21-25, 27, 29-39, 48-63

queue 1, threshold 2: 12, 20, 28

queue 1, threshold 3: 10, 18, 26

queue 8, threshold 1: 40-47

Additional Information:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/qos.html

- Number of login retries for user authentication is configurable

  **Old behavior:** If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple login retries.

  **New behavior:** The number of login retries is configurable. The default number of retries is 5.

  **Additional information:**

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_auth/configuration/15-2mt/sec-cfg-authen-prxy.html#GUID-ED4C668A-3E5F-44BE-83CF-A3B490E5AEDF

- IOS Server Load Balancing (SLB) CLI removal

  **Old behavior:** Release 12.2(33)SXI and rebuilds and earlier releases support IOS SLB.

  **New behavior:** IOS SLB is not supported in Release 12.2(33)SXJ and later releases. The IOS SLB CLI is not present in Release 12.2(33)SXJ3 and later releases.

  **Additional information:** Release 12.2(33)SXJ and later releases support server load balancing (SLB) as implemented on the Application Control Engine (ACE) module (ACE20-MOD-K9).

# Cisco IOS Release 12.2(33)SXI12

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXI12.

# Cisco IOS Release 12.2(33)SXI11

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXI11.

# Cisco IOS Release 12.2(33)SXI10

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXI10.

# Cisco IOS Release 12.2(33)SXI9

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI9:

- Uncorrectable adjacency table ECC error response

  **Old Behavior:** When an uncorrectable adjacency table ECC error occurs, a message was generated.

**New Behavior:** You can configure the reponse to an uncorrectable adjacency table ECC error as either a message (default) or module reset and a message.

**Additional Information:** Enter the **mls cef error adjacency ecc-uncorrectable action reset** global configuration mode command to configure module reset as the reponse to an uncorrectable adjacency table ECC error. Enter the **no mls cef error adjacency ecc-uncorrectable action reset** global configuration mode command to revert to the default behavior (generate a message as the reponse to an uncorrectable adjacency table ECC error).

- Number of login retries for user authentication is configurable.

  **Old Behavior:** If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple login retries.

  **New Behavior:** The number of login retries is configurable. The default number of retries is 5.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_auth/configuration/15-2mt/sec-cfg-authen-prxy.html#GUID-ED4C668A-3E5F-44BE-83CF-A3B490E5AEDF

# Cisco IOS Release 12.2(33)SXI8a

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXI8a.

# Cisco IOS Release 12.2(33)SXI8

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI8:

- CSM module configuration synchronization

  **Old Behavior:** In releases where CSCtj44456 is not resolved, the **hw-module csm slot_number standby config-sync** command can be entered even if the CSM configuration is being modified in another administrative session.

  **New Behavior:** In releases where CSCtj44456 is resolved, a message is displayed and the **hw-module csm slot_number standby config-sync** command does not take effect if the CSM configuration is being modified in another administrative session.

  **Additional Information:** None.

# Cisco IOS Release 12.2(33)SXI7

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI7:

- BGP No Longer Activates IPv6 Peers in IPv4 Address Family Automatically

  **Old Behavior:** By default, both IPv6 and IPv4 capability is exchanged with a BGP peer that has an IPv6 address. When an IPv6 peer is configured, that neighbor is automatically activated under the IPv4 unicast address family.

  **New Behavior:** Starting with new peers being configured, an IPv6 neighbor is no longer automatically activated under the IPv4 address family. You can manually activate the IPv6 neighbor under the IPv4 address family if you want. If you do not want an existing IPv6 peer activated under

the IPv4 address family, you can manually deactivate the peer with the no neighbor ipv6-address activate command. Until then, existing configurations that activate an IPv6 neighbor under the IPv4 unicast address family will continue to try to establish a session.

**Additional Information:**

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/12-2sx/irg-basic-net.html

- Change in transceiver detail show command output

  **Old Behavior:** The **show interfaces tengigabitethernet** *slot*/*port* **transceiver detail** command voltage fields display **0.00** for all outputs.

  **New Behavior:** The voltage fields display **N/A** for all outputs.

  **Additional Information:** None.

- IEEE 802.1X Enhancement

  **Old Behavior:** Not applicable

  **New Behavior**: Addition of the optional **delay** *delay_interval* keyword and argument:

  ```
  Router(config)# ip device tracking [probe {count count | delay delay_interval | interval interval}]
  ```

  Configures these parameters for the IP device tracking table:

  *count*—Number of times that the switch sends the ARP probe. The range is 1 to 5. The default is 3.

  *delay_interval* (implemented in releases where CSCtn27420 is resolved)—Number of seconds that the switch delays sending an ARP probe, triggered by link-up and ARP probe generation by the tracked device. The range is 1 to 120 seconds. The default is 0 seconds.

  *interval*—Number of seconds that the switch waits for a response before resending the ARP probe. The range is 30 to 300 seconds. The default is 30 seconds.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#CSCtn27420

- IP DHCP snooping enhancements

  **Old Behavior:** not applicable

  **New Behavior:** Release 12.(33)SXI7 has these IP DHCP snooping CLI changes.

  ```
  Router(config)# ip dhcp snooping information option replace
  ```

  Or:

  ```
  Router(config-if)# ip dhcp snooping information option replace
  ```

  Replaces the DHCP relay information option received in snooped packets with the switch's option-82 data. Available in releases where CSCto29645 is resolved and when DHCP option-82 data insertion is enabled.

  ```
  Router(config-if)# ip dhcp snooping information option allow-untrusted
  ```

  Available in interface configuration mode in releases where CSCto29645 is resolved.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snoodhcp.html#CSCto29645

# Cisco IOS Release 12.2(33)SXI6

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI6:

- BFD CPU Utilization

  **Old Behavior:** CPU Hog is reported by BFD PP process and initial research shows it could be an issue with process's hog detection and bailout. There were no macros supporting the process hog detection and bailout.

  **New Behavior:** Two new macros have been added to the support process hog detection and bailout.

- Persistence for SNMP Engine ID

  **Old Behavior:** SNMP Engine ID persistence is not available

  **New Behavior:** SNMP Engine ID persistence is available. The Engine ID is stored in the NVRAM, the first time when it is generated. The Engine ID is written to a file called snmpid-file in the NVRAM. This file is created in active Route Processor(RP) when you use the write memory command or the copy running startup command. The file will be created in the standby RP when the Engine ID is synced to the standby RP.

  If the file exists in NVRAM, the Engine ID persistence is guarenteed. If this file is removed for some reason and device is reloaded, the following message is displayed on the console on bootup-00:01:37: % SNMP ID Persistence Error : Unable to open file : No such file or directory

  The persistence is only for the default SNMP Engine ID. If you have configured the Engine ID using the snmp-server engineID local command, then that Engine ID will have precedence over the persisted Engine ID.

- The summary address is not advertised to the peer

  **Old Behavior:** The summary address is advertised to the peer if the administrative distance is configured as 255.

  **New Behavior:** The summary address is not advertised to the peer if the administrative distance is configured as 255.

- Fan tray messages for failure and absence

  **Old Behavior:** Except for E-series chassis, the message displayed for either a fan tray failure or for removal reported only failure or absence (different causes were reported in different releases).

  **New Behavior:** Except for E-series chassis, the message displayed for either a fan tray failure or for removal reports that the cause might be either a failure or absence.

# Cisco IOS Release 12.2(33)SXI5

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI5:

- Source IP address sent in prune echo messages is now set to the source IP address of the prune echoer

  **Old Behavior:** The source IP address of prune echo messages is not set to the source IP address of the router that is echoing the prune message (prune echoer). This behavior is not in accordance with RFC 4601 and could potentially cause interoperability issues in certain IPTV deployment scenarios, for example, in VPLS deployments with a mix of Cisco and third-party routers.

  **New Behavior:** The source IP address that is sent in prune echo messages is now set to the source IP address of the prune echoer.

  **Additional Information:** None.

- New CLI option is added to view the running configuration without the ACL information.

  **Old Behavior:** The ACL information is displayed in the running configuration .

  **New Behavior:** The show running command is modified to provide an option to view the running configuration without the ACL information.

  **Additional information:**

  http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_s5.html#show_running-config

- SPAN restrictions in PFC3B modes with **xconnect encapsulation mpls**

  **Old Behavior:** In PFC3B mode or PFC3BXL mode, the **xconnect encapsulation mpls** command might cause traffic to loop continuously with these SPAN configurations:

  – To avoid the problem, if the **xconnect encapsulation mpls** command is configured on a physical interface, the CLI prevents configuration of that port as part of a SPAN session.

  – To avoid the problem, if a SPAN session is configured on a physical port and you attempt to configure the **xconnect encapsulation mpls** command, the CLI prints a warning that recommends against the configuration.

  – If the **xconnect encapsulation mpls** command is configured on a physical interface, you should not configure **source cpu** {**rp** | **sp**} in any SPAN session, but the CLI does not enforce any restriction.

  – If a SPAN session is configured with **source cpu** {**rp** | **sp**} and you attempt to configure the **xconnect encapsulation mpls** command, the CLI does not enforce any restriction.

  **New Behavior:** In releases where CSCth62957 is resolved, to avoid a configuration that might cause traffic to loop continuously, the CLI enforces these restrictions in PFC3B mode or PFC3BXL mode:

  – If the **xconnect encapsulation mpls** command is configured on a physical interface, the CLI prevents configuration of that port as part of a SPAN session.

  – If a SPAN session is configured on a physical port and you attempt to configure the **xconnect encapsulation mpls** command on that port, the CLI prints a warning that recommends against the configuration.

  – If the **xconnect encapsulation mpls** command is configured on a physical interface, you cannot configure **source cpu** {**rp** | **sp**} in any SPAN session.

  – If a SPAN session is configured with **source cpu** {**rp** | **sp**} and you attempt to configure the **xconnect encapsulation mpls** command, the CLI prints a warning that recommends against the configuration.

  **Additional Information:** None.

- Support for the **exception switch kernel** command

  **Old Behavior:** Releases 12.2(33)SXI4 and 12.2(33)SXI4a support the **exception switch kernel** command.

  **New Behavior:** Release 12.2(33)SXI5 and later releases do not support the **exception switch kernel** command.

  **Additional Information:** None.

# Cisco IOS Release 12.2(33)SXH8b

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXH8b.

# Cisco IOS Release 12.2(33)SXH8a

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXH8a.

# Cisco IOS Release 12.2(33)SXH8

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXH8:

- TM_DATA_PARITY_ERROR error, ASIC reset, and supervisor engine reload

  **Old Behavior:** The response to an TM_DATA_PARITY_ERROR error was an ASIC reset and interrupted inband traffic.

  **New Behavior:** The response to an TM_DATA_PARITY_ERROR error is a supervisor engine reload.

  **Additional Information:**

  http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtf51541

- Option to automatically unconfigure the FTP, TFTP, an RCP source interface configuration.

  **Old Behavior:** The FTP, TFTP, an RCP source interface configuration needs to be manually unconfigured.

  **New Behavior:** The FTP, TFTP, an RCP source interface configuration is now automatically unconfigured. This helps to prevent any router crash if the source interface configurations are utilised further unknowingly.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_cfg_ser_if.html

- Duplicate remark statements can no longer be configured from the IPv6 access control list.

  **Old Behavior:** Duplicate remark statements could be configured from the IPv6 access control list.

  **New Behavior:** Duplicate remark statements can no longer be configured from the IPv6 access control list. Because each remark statement is a separate entity, each one is required to be unique.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_05.html

- TestAclFpgaMonitor Diagnostic

  **Old Behavior:** The TestAclFpgaMonitor diagnostic was not supported.

  **New Behavior:** The TestAclFpgaMonitor diagnostic is supported.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-41A39BF2-A0F6-434D-A49C-BFDE3285D01E

- Supervisor engine response to a major alarm

  **Old Behavior:** With redundant supervisor engines, the redundant supervisor engine becomes active and the active supervisor engine drops to ROMMON. With a single supervisor engine, if the cause of the major alarm is not corrected, after 5 minutes the supervisor engine drops to ROMMON.

  **New Behavior:** With redundant supervisor engines, the redundant supervisor engine becomes active and the active supervisor engine drops to ROMMON. In releases where CSCtf54909 is resolved, if the fan tray is faulty or absent, the active supervisor engine shuts down. With a single supervisor

engine, if the cause of the major alarm is not corrected, after 5 minutes the supervisor engine drops to ROMMON. In releases where CSCtf54909 is resolved, if the fan tray is faulty or absent, the supervisor engine shuts down.

- TestScratchRegister Added to Online Diagnostics

  **Old Behavior:** Online diagnostics did not test the scratch register for SPAs in 7600-SIP-200 or 7600-SIP-400.

  **New Behavior:** The "TestScratchRegister" test is implemented in online diagnostics for SPAs in 7600-SIP-200 and 7600-SIP-400.

# Cisco IOS Release 12.2(33)SXH7

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXH7:

- MTU on PA-1FE and PA-2FE port adapters

  **Old Behavior:** MTU is not configurable on PA-1FE and PA-2FE port adapters. When a you attempted to configure the interface MTU, the following message was printed:

  ```
  % Interface {Interface Name} does not support user settable mtu
  ```

  **New Behavior:**You can configure the interface MTU on PA-1FE and PA-2FE port adapters (PAs).

  **Additional Information:** See the *MPLS MTU Command Changes* document at the following URL:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_mtu_cmd_changes.html

- IPv6 packets with extension headers

  **Old Behavior:** IPv6 packets with extension headers are processed in hardware.

  **New Behavior:** In releases where CSCtc71597 is resolved, to address the issues described in CSCtc71597, you can enable software processing of IPv6 packets with extension headers. If your IPv6 traffic does not specify a L4 protocol, software processing of IPv6 packets with extension headers is unnecessary. If your IPv6 traffic specifies a L4 protocol, enable software processing of IPv6 packets with extension headers.

  **Additional Information:** Enter the **platform ipv6 acl punt extension-header** global configuration command to enable software processing of IPv6 packets with extension headers.

  Enter the **mls rate-limit unicast acl input 100 pps** command to limit the number of packets sent to the RP for processing in software.

- NTP mode 7 packet processing

  **Old Behavior:** Cisco IOS Software releases process NTP mode 7 packets.

  **New Behavior:** Cisco IOS Software releases where CSCtd75033 is resolved do not process NTP mode 7 packets, and instead, if debugs for NTP are enabled, display "NTP: Receive: dropping message: Received NTP private mode packet. 7".

  **Additional Information:** To have Cisco IOS Software process NTP mode 7 packets, enter the **ntp allow mode private** command (disabled by default).

# Cisco IOS Release 12.2(33)SXH6

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXH6:

- Dynamic NAT entries do not time out correctly in certain cases.

  **Old Behavior:** If NAT was configured with the ip nat translation max-entries command and the limit was reached, incoming packets could not create any new entries in a NAT table. To remedy this situation, packets were sent to the process path. Eventually, the packets sent to the process path were dropped. This behavior caused a high CPU usage problem.

  **New Behavior:** Packets received after the max-entries limit has been reached are dropped at the CEF path.

  **Additional Information:** None.

- CLI change to bgp aggregate-timer command to suppress more specific routes

  **Old Behavior:** More specific routes are advertised and withdrawn later, even if aggregate-address summary-only is configured. The BGP table shows the specific prefixes as suppressed.

  **New Behavior:** The bgp aggregate-timer command now accepts the value of 0 (zero), which disables the aggregate timer and suppresses the routes immediately.

  **Additional Information:** None.

- Update show environment status command to include power input 4

  **Old Behavior:** In releases where CSCtb57321 is not resolved, the show environment status output displays power inputs 1-3 but not 4.

  **New Behavior:** In releases where CSCtb57321 is resolved, all 4 power inputs are displayed.

  **Additional Information:** None.

- New option, (**exclude vlan**) is added for **port-channel load-balance** command for PFC3C mode chassis.

  **Old Behavior:** There is no option to exclude VLAN in the IP-related load distribution.

  **New Behavior:** The **exclude vlan** option is added for IP-related load balance methods such as **dst-ip**, **dst-mixed-ip-port**, **src-dst-ip**, **src-dst-mixed-ip-port**, **src-ip**, and **src-mixed-ip-port**. Using this option excludes the VLAN in the IP-related load distribution.

  **Additional Information:**
  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-o1.html#GUID-464753DB-036E-4225-9AF9-2580245E747E

- New CLI allows VACL capture of software-switched WAN packets

  **Old Behavior:** Software-switched WAN packets are not subjected to ACL lookup in the ACL TCAM and are therefore not affected by hardware-only features. As a result, VACL capture will fail for software-switched WAN packets.

  **New Behavior:** The platform cwan acl software-switched command allows software-switched WAN packets to be subjected to ACL lookup, and VACL capture will capture software-switched WAN packets. The show platform acl software-switched command displays the state of this feature.

  **Additional Information:**
  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.html#VACL_Configuration_Guidelines

- New command (**mls ip slb purge global**) no longer causes ISSU failure

**Old Behavior:** When you perform an ISSU to a new version that introduces support for the **mls ip slb purge global** command, the command, which is enabled by default, appears in the generated configuration. During the ISSU **runversion** phase, when the updated active device attempts to synchronize configuration with the standby device, the standby device does not recognize the **mls ip slb purge global** command, and the ISSU fails.

**New Behavior:** The **mls ip slb purge global** command, which is enabled by default, does not appear in the generated configuration unless the configuration disables the feature. When you perform an ISSU to a new version that introduces support for the **mls ip slb purge global** command, the new command will not appear in the running configuration or generated configuration and will not cause an ISSU failure.

- Loopback interfaces are shut down on dual-active detection

  **Old Behavior:** An active chassis that detects a dual-active condition shuts down all of its non-VSL physical interfaces except interfaces configured to be excluded from shutdown. Loopback interfaces are not shut down.

  **New Behavior:** An active chassis that detects a dual-active condition shuts down all of its non-VSL physical and loopback interfaces except interfaces configured to be excluded from shutdown.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Recovery_Actions

- Support for the VLAN translation on ME6500 switches and WS-X6148A-GE-TX switching modules

  **Old Behavior:** In releases where CSCsy34566 is not resolved, the VLAN translation CLI is available on ME6500 switches and WS-X6148A-GE-TX switching modules, but does not function correctly.

  **New Behavior:** In releases where CSCsy34566 is resolved, the VLAN translation CLI is not available on ME6500 switches and WS-X6148A-GE-TX switching modules.

  **Additional Information:** None.

- Support for the **mls cef tunnel fragment** command in PFC3A and PFC3B modes

  **Old Behavior:** In releases later than 12.2(18)SFX and rebuilds, the **mls cef tunnel fragment** command is not supported in PFC3A and PFC3B modes.

  **New Behavior:** In releases where CSCsy69228 is resolved, the **mls cef tunnel fragment** command is supported in PFC3A and PFC3B modes.

  **Additional Information:**
  http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_i1.html#mls_cef_tunnel_fragment

- New CLI allows VACL capture of software-switched WAN packets

  **Old Behavior:** Software-switched WAN packets are not subjected to ACL lookup in the ACL TCAM and are therefore not affected by hardware-only features. As a result, VACL capture will fail for software-switched WAN packets.

  **New Behavior:** The platform cwan acl software-switched command allows software-switched WAN packets to be subjected to ACL lookup, and VACL capture will capture software-switched WAN packets. The show platform acl software-switched command displays the state of this feature.

  **Additional Information:**
  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.html#VACL_Configuration_Guidelines

- Added support for the **powerdown** keyword on the **environment-monitor shutdown temperature** command for the Catalyst 6500 switches.

  **Old Behavior:** In releases where CSCtb58571 is not resolved, when a major temperature alarm is detected on the active supervisor engine, the system is forced to ROMMON.

  **New Behavior:** In releases where CSCtb58571 is resolved, when a major temperature alarm is detected on the active supervisor engine, the system is forced to ROMMON only if configured with the **rommon** keyword. If the **powerdown** keyword is configured then the active supervisor is powered down.

  **Additional Information:** None.

- Support added to actively detect the rogue DHCP Servers.

  **Old Behavior:** None of the old behavior has been changed. Additional feature has been introduced.

  **New Behavior:** DHCPDISCOVER messages will be sent out on untrusted ports and when the response comes back they are logged. User needs to specify list of VLANs on which the spurious DHCP server detection is required. The messages will be simultaneously sent out on all untrusted ports belonging to those VLANs at a configurable interval. The source MAC address of DHCPDISCOVER messages will be that of the switch.

  The enhanced logging will trigger syslog for DHCPOFFER, DHCPACK, DHCPNAK, DHCPLEASEQUERY messages on untrusted ports. There are no trigger mechanisms on trusted ports. These syslogs will be rate-limited.

  Further all the responses for bogus messages will be logged in a database. The database will not be persistent across a reload/SSO. CLI will be provided to clear the database. Database fields will include MAC + IP + VLAN + Interface + Last Seen + Count.

  **Additional Information:** None.

# Cisco IOS Release 12.2(33)SXH5

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXH5:

- RPF check behavior changed when an RPF neighbor is learned via BGP

  **Old Behavior:** When a potentially better RPF neighbor is learned via BGP and PIM hellos from that RPF neighbor have not been received over the MDT tunnel, the RPF check will fail resulting in traffic loss because the RPF interface is set to NULL.

  **New Behavior:** When a potentially better RPF neighbor is learned via BGP and PIM hellos from that RPF neighbor have not been received over the MDT tunnel, the RPF check will set the RPF interface to the MDT tunnel instead of NULL, thereby preventing traffic loss.

  **Additional Information:** None.

- DHCP: Ports UDP 67 and 68 are now closed in the Cisco IOS DHCP/BOOTP default configuration.

  **Old Behavior:** DHCP services are enabled by default and ports UDP 67 and 68 are open in the Cisco IOS DHCP/BOOTP default configuration.

  **New Behavior:** There are now two logical parts to the **service dhcp** command: **service enabled** and **service running**. The DHCP service is enabled by default, but port 67 (the server port) is not opened until the DHCP service is running. Port 68 (the DHCP client port) is closed by default when a router loads. The client port is opened when certain DHCP processes start.

  **Additional information:**

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-2sx/config-dhcp-server.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-2sx/config-dhcp-client.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-r1.html#GUID-1516B259-AA28-4839-B968-8DDBF0B382F6

- DHCP: the renew deny unknown DHCP pool configuration command configures the DHCP server renewal policy for unknown DHCP clients.

  **Old Behavior:** The DHCP server ignores a client request for an IP address that is not currently leased to the client.

  **New Behavior:** If the DHCP server is configured to secure ARP table entries to DHCP leases and the renew deny unknown command is configured, the DHCP server can acknowledge the request and start the process of lease negotiation with the client.

  **Additional information:**

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-mt/config-dhcp-accounting-security.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-r1.html#GUID-1516B259-AA28-4839-B968-8DDBF0B382F6

- **snmp mib flash cache** command introduced.

  **Old Behavior:** No cache was maintained for CISCO-FLASH-MIB.

  **New Behavior:** The **snmp mib flash cache** command has been added to start a process that constructs and maintains a cache.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_17.html#snmp_mib_flash_cache

- SNMP query for **cdpCacheAddress** provides a global unicast IPv6 address.

  **Old Behavior:** The SNMP query for **cdpCacheAddress** provided a link-local IPv6 address.

  **New Behavior:** SNMP query for **cdpCacheAddress** provides a global unicast IPv6 address.

  **Additional Information:** None.

- Default Change

  **Old Behavior:** The maximum value of **queue-depth hello** and **queue-depth update** is displayed as 4294967295.

  **New Behavior:** The maximum value of **queue-depth hello** and **queue-depth update** is changed to 2147483647.

  **Additional Information:**

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_q1.html#queue-depth

- CLI output change for **show ip traffic** command.

  **Old Behavior:** The **show ip traffic** command displays the ARP (proxy) reply counter as the number of ARP replies for real proxies and for virtual IP addresses.

  **New Behavior:** The **show ip traffic** command displays the ARP (proxy) reply counter as the number of ARP replies for real proxies only.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios/ipapp/command/reference/iap_s2.html#show_ip_traffic

- CLI change for bidirectional forwarding detection (BFD).

  **Old Behavior:** Cisco IOS software incorrectly allows for configuration of BFD on virtual-template and virtual-access (dialer) interfaces.

  **New Behavior:** Cisco IOS software no longer allows configuration of BFD on these types of interfaces.

  **Additional information:**

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/12-2sx/irb-12-2sx-book.html

- For a virtual switch (VS), the **show tech-support** command now includes information about the active and standby switches.

  **Old Behavior**: When the **show tech-support** command is entered on a virtual switch (VS), the command output includes the output of the **show module** command and the **show power** command for only the active switch.

  **New Behavior:** When the **show tech-support** command is entered on a virtual switch (VS), the command output includes the output of the **show module** command and the **show power** command for both the active and standby switches.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios/vswitch/command/reference/vs_book.html

  http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_s4.html#show_tech-support

- **ip-sec manual** keyword not supported by the VPN SPA.

  **Old Behavior:** When the **ipsec-manual** keyword is entered, the following message appears beneath the entry line: “This new crypto map will remain disabled until a peer and a valid access list have been configured.”

  **New Behavior:** The **ipsec-manual** keyword is not supported by the VPN SPA. If the **ipsec-manual** keyword is entered, the following error message appears beneath the keyword entry line: “Manually-keyed crypto map configuration is not supported by the current crypto engine.” The change is only to the message printed. Manual keying for the VPN SPA was removed.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html#crypto_map_(global_IPSec)

- Supported interfaces are now described in the **bfd** command.

  **Old Behavior:** BFD supported interfaces were not listed in the **bfd** command.

  **New Behavior:** Supported interfaces are now listed in the **bfd** command. The supported interfaces are Ethernet, Serial, Frame Relay, ATM, and dot1q vlan subinterfaces (with IP address on the dot1q subinterface). A note has been added to the **bfd** command documentation that states that other interfaces are not supported by BFD.

**Additional Information:**

http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#bfd

- CLI behavior change for **show etherchannel** and **port-channel port load defer** commands.

  **Old Behavior:** When a port is activated as part of an EtherChannel, the load share and LTL/FPOE are computed and programmed in the hardware immediately. When activation occurs during recovery of a dropped connection to a failed VSS chassis, data loss occurs, especially for multicast traffic, because the VSS chassis is not immediately ready to receive data.

  **New Behavior:** The **show etherchannel port-channel** command is updated to display the new information provided by the **port-channel port load-defer** command syntax. By enabling the newly added **port load share deferral** feature, the load share and LTL/FPOE programming of a port are deferred for a period configurable by the user. Two new CLI commands are added: the **new port-channel port load-defer** command enables the feature on a port channel and the new **port-channel load-defer** command allows configuration of the deferral period. New fields are added to the **show etherchannel** command to display the feature configuration and state.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-cr-book_chapter_010001.html#wp2089533070

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-o1.html#GUID-13F4C686-1A5A-4689-B33C-1FDDC4B1D932

- New syslog message when VLAN addition fails.

  **Old Behavior:** When the user attempts to add a VLAN to the VLAN database, no syslog message is sent if the operation fails.

  **New Behavior:** When a VLAN cannot be added to the VLAN database, the following syslog message is sent:

  ```
  %SW_VLAN-4-VLAN_ADD_FAIL: Failed to add VLAN [dec] to vlan database: [chars]
  ```

  The user is now alerted to the condition and can investigate the cause.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/ios/12_2sx/system/messages/sm2sx09.html#SW_VLAN-4

- The **TestL3HealthMonitoring** diagnostic no longer runs automatically.

  **Old Behavior:** The **TestL3HealthMonitoring** diagnostic default automatic run setting is **enabled**.

  **New Behavior:** The **TestL3HealthMonitoring** diagnostic default automatic run setting is **disabled**. The diagnostic can be enabled by the user after the module is online.

  **Additional Information:**

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/diagtest.html#TestL3HealthMonitoring

# Restrictions

These sections list restrictions for Cisco IOS for the Catalyst 6500 series switches:


- Restrictions Removed by the PFC3, page 207
- General Limitations and Restrictions, page 207


## Restrictions Removed by the PFC3

The PFC3 removes these restrictions that were present with other policy feature cards:

- You can configure features to use up to 3 different flow masks.
- You can configure more than 1 Gateway Load Balancing Protocol (GLBP) group.
- You can configure up to 255 unique HSRP group numbers.
- You can configure a separate MAC address on each interface.
- You can configure Unicast RPF check without reducing the number of available CEF entries.
- You can configure VLAN-based QoS with DFC3s installed.
- You can configure port-based and VLAN-based QoS on a per-port basis on the WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules.
- You can configure QoS policy maps attached to an EtherChannel formed from interfaces on different DFC-equipped switching modules.

## General Limitations and Restrictions

This section describes general limitations and restrictions:

| Identifier | Technology | Description |
|---|---|---|
| CSCeb06765 | — | Request for Global command to enable Syslog |
| CSCec27709 | — | HSRP/VRRP/GLBP switchover delays with switchports on DFC3A |
| CSCec79733 | — | VPN-SM-C2:Ingress traffic on Intf vlan cannot be spanned |
| CSCed76016 | — | traceback message when boot up from sup720 |
| CSCef12458 | — | SNMP topology discovery caused Cat6000 high CPU utilization |
| CSCef19599 | — | Service policy marking inbound not working on SUP720 |
| CSCek39668 | — | Need to port the fix of CSCsb58066 to cat6000/c7600 platform codes |
| CSCsb59015 | — | L3 packet duplication with vacl capture enabled and WS-X6708 present |
| CSCse07679 | — | Multicast with L2 broadcast address is routed w/o rewriting the mac. |
| CSCse86399 | — | PBR forwards local destined packets which match ACL criteria |
| CSCsl86574 | — | Some commands are not getting converted when converting vs to standalone |
| CSCsm43234 | — | %ISSU_PROCESS-SP-3-SYSTEM: Not enough space in NVRAM;Fail to set bootvar |
| CSCsw67926 | — | C2W2: CFM Draft1 does not support in Whitney2.0. |
| CSCsx11253 | — | Traceback@ip_adm_ha_cf_get_msg_buf during reauthentication with webauth |

| Identifier | Technology | Description |
|---|---|---|
| CSCsy31055 | — | Support for patching modular IOS images deferred |
| CSCtc10254 | — | IPv6 raguad fail to drop RA pkt with hop-by-hob and auth ext hdr |
| CSCte31168 | — | CFM:W2.C-->SXI1 with cfm configs, 2MR LCs are powered down |
| CSCtf08313 | — | Authentication doesnt start with traffic on link up.(Multi-auth) |
| CSCtf18029 | — | MPLS ENF-ISSU : Internal VLAN not removed on downgrade |
| CSCtf32483 | — | CSM not loadbalancing when a real is removed/added dynamically |
| CSCtf41722 | — | W2.Clix:Multicast Service Reflect: Translation Entries missing in DFCs |
| CSCtf48652 | — | W2.Clix: service reflection with short masks requires rate-limit tweak |
| CSCtf48659 | — | W.Clix: missing OIF in rmcast Serv Refl with BIDIR in priv network |
| CSCtf51285 | — | W2.Clix: after switchover, some groups miss ServRefl. vlans in OIF-list |
| CSCtg14082 | — | W2.Clix: shutdown of VSL link causes 80 seconds mcast disruption |
| CSCtg17528 | — | c2w2c: fast redirect broken on secondary portchannel id's (still) |
| CSCtg33528 | — | 10G SFP+: Some fields in the o/p of 'sh idprom interface' shows unspecif |
| CSCtg61862 | — | Vacl capture stops on reloading legacy card. |
| CSCtg89884 | — | "%FABRIC-SP-6-TIMEOUT_ERR" upon ISSU SXI4-->SXI2a, powering up the LCs |
| CSCth03423 | — | Standby Sup crashes due to bulk sync failure, Issue same as CSCsx46323 |
| CSCti98129 | — | rcv queue bandwidth does not programmed in sh qm port for R2D2 rev2 |
| CSCtj16159 | — | standby reboots twice and comes up in rpr due to config sync fail |
| CSCtj27150 | — | Module 1. LCC Client UNSOLICITED SCP failed |
| CSCtj41404 | — | Tracebacks at pm_port_want_to_bundle on shut/noshut on range of mlacp po |
| CSCtj41777 | — | multicast traffic drop and duplicate - DR reload |
| CSCtj46469 | — | C2WA1:Ports succesfully budled in sec agg flap on modifying Po VLAN mask |
| CSCtj49906 | — | Marking does not work with CoPP policy |
| CSCtk76193 | — | ES40 QoS : No more than 7 classes accepted on a policy-map (Flat/HQoS) |
| CSCtl03171 | — | c2wa1:Periodic High CPU due to SNMP ENGINE process with NAM in VSS setup |
| CSCtl06114 | — | SGT is not assigned to webauth client even after receiving from ACS |
| CSCtl69556 | — | block qos config on portchannel with same asic as vsl on load/issu |
| CSCtn45851 | — | Fail to achieve more then 5gig through put on 2VTI Tunnel in VSS |
| CSCtn77625 | — | ES40 QoS : cos2exp service-policy command missing in run-confg on reload |
| CSCto66065 | — | NAM3: hw-module shutdown cmd power down NAM3 |
| CSCto85304 | — | c2wa1b: ERSPAN monitoring fails when routed src port is on CFC on VSS |
| CSCtq23239 | — | ES40 Interface not coming UP on reload of VSS |
| CSCtq90786 | — | c2wa1b:RG doesn't re-calc sys-id on changing mlacp sys-prio on a PoA |
| CSCtq95747 | — | NAM3:dataport 2 not rcv traffic if same span destined to both dataports |
| CSCtt16904 | — | c2wa1c: memory leak when bennu and nam are reset together. |
| CSCtt43196 | — | L3 Multicast stream over VPLS affected by Link down |
| CSCtu26761 | — | c2wa1c: Bennu states toggles due to autostate down on VSS |

| Identifier | Technology | Description |
|---|---|---|
| CSCtu34830 | — | VPLS_TE_FRR_Multicast traffic is affected |
| CSCtw53269 | — | SXJ2:standby reloads twice @%SATVS_IBC-SW1_SP-5-VSL_DOWN_SCP_DROP |
| CSCty26003 | — | LTL index missing post sso+rcfg (no functionality or traffic impact) |
| CSCub47529 | — | Enhanced FlexWAN (WS-X6582-2PA) silently reload during BERT w/o crashinf |
| CSCdx10583 | Cisco IOS | EoMPLS:CWPA: per-vlan shaping does not work when egress is FlexWan |
| CSCdx39882 | Cisco IOS | hubble: SNMP traps delayed 3-10 minutes |
| CSCea53554 | Cisco IOS | const2: C2MSFC3: PBR continues to fwd traffic when RPF check fails |
| CSCea70203 | Cisco IOS | eigrp dflt-network stays prg in h/w when route is removed |
| CSCeb01860 | Cisco IOS | Const2:egress qos policy applied to ingressing rpf failure pkts |
| CSCec02266 | Cisco IOS | Berytos perf drop if sw reboot after NVRAM is cleared |
| CSCed29392 | Cisco IOS | MPLS: Egress ACL applied on tagged traffic |
| CSCee39455 | Cisco IOS | Sporadic packet drops on 6704 linecard under IPv6 Unicast Bidir flows |
| CSCef08631 | Cisco IOS | MVPN: multicast entries in globle table leak into VRF table |
| CSCef78235 | Cisco IOS | Disable egress span of vacl redirected packets |
| CSCeg29898 | Cisco IOS | MMLS: rpdf-cache not updated when using BSR. Bidir flows SW switched |
| CSCsb25509 | Cisco IOS | eibgp load balancing interwork with tag to ip recirculation cause loop |
| CSCtc91284 | Infrastructure | W2C: polling flashMIB shows wrong info with snmp mib flash cache enabled |
| CSCtc06369 | IPServices | NAT source address translation not done for PIM register packets |
| CSCtd72233 | IPServices | Able to disable IPv6 with HSRPv6 configured and the state is active |
| CSCtl73810 | IPServices | c2wa1:ISSU from SXI4a/SXI4 to later image fails due to RF progression |
| CSCsg08736 | LegacyProtocols | @SyncMutexLock_r - Blocked remote registry call from blob to ION pro |
| CSCee77417 | MPLS | TE/FRR:FRR broken when LDP NOT enabled |
| CSCds22281 | platform-cat6xxx | ip multicast rate-limit command inadvertently removed from config |
| CSCdt72147 | QoS | microflow policing not working with same flow on multiple input port |
| CSCtf14368 | Routing | sh runn VRF does not show EIGRP vrf config |
| CSCtg60341 | Routing | IPv6 stalled interface is sending HSRP-Hellos |
| CSCtk63987 | Routing | c2wa1: crash in pdb_flushcache during unconfig |
| CSCec29255 | WAN | Flexwan OIR causes WS-6516-GBIC (no DFC) to reload |

- When a redundant supervisor engine is in standby mode, the Ethernet ports on the redundant supervisor engine are always active.
- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannel (maximum of eight interfaces) with no requirement that the ports be contiguous.
- All Ethernet ports on all modules support 802.1Q VLAN trunking.
- When you add a member port that does not support ISL trunking to an EtherChannel, Cisco IOS software automatically adds a **switchport trunk encapsulation dot1q** command to the port-channel interface to prevent configuration of the EtherChannel as an ISL trunk. The **switchport trunk encapsulation dot1q** command is inactive when the EtherChannel is not a trunk.

- A distributed EtherChannel (DEC) is an EtherChannel with ports on more than one DFC-equipped module or, on a DFC-equipped dual-fabric connection module, with ports that use different fabric connections. (Search for "Dual switch-fabric connections" in this document.)
- To reduce CPU utilization during ACL configuration changes, use named ACLs instead of numbered ACLs whenever possible, because the ACL merge algorithm runs each time you change an ACE in a numbered ACL. With named ACLs, the ACL merge algorithm runs only when you exit the named ACL configuration mode.
- In releases where caveat CSCef78235 is resolved, with any Supervisor Engine 720 hardware revision, local SPAN and RSPAN source ports do not copy VACL-redirected traffic.

  In releases where caveat CSCef78235 is not resolved:

  - With WS-SUP720, hardware revision 3.2 or higher, local SPAN source ports do not copy VACL-redirected traffic.
  - With WS-SUP720 hardware revisions lower than 3.2, local SPAN source ports copy VACL-redirected traffic.
  - With any Supervisor Engine 720 hardware revision, RSPAN source ports copy VACL-redirected traffic.

  Enter the **show module version | include WS-SUP720-BASE** command to display the hardware revision. For example:

```
Router# show module version | include WS-SUP720-BASE
 7    2  WS-SUP720-BASE     SAD075301SZ Hw :3.2
```

- IPsec in software on the MSFC is supported only for administrative connections to Catalyst 6500 series switches and Cisco 7600 series routers.
- PFC QoS does not rewrite the payload ToS byte in tunnel traffic.
- PFC QoS does not rewrite the ToS byte in bridged multicast traffic.
- The PFC3 does not apply egress policing to traffic that is being bridged to the MSFC3.
- The PFC3 does not apply egress policing or egress DSCP mutation to multicast traffic from the MSFC3.
- The MSFC3 supports tunnels configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT (for inside to outside translation), TCP intercept, context-based access control (CBAC), and encryption.
- The PFC3A does not support any PFC QoS features on tunnel interfaces.
- The PFC3BXL does not provide hardware switching for ICMP traffic if you configure NAT.
- The PFC3A does not provide hardware switching for ICMP traffic if you configure NAT or Cisco IOS reflexive ACLs.
- If you have a network device in your network with MAC address reduction enabled, you should also enable MAC address reduction on all other Layer-2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

  When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With MAC address reduction enabled, a switch bridge ID (used by the spanning-tree algorithm to determine the identity of the root bridge, the lowest being preferred) can only be specified as a multiple of 4096. Only the following values are possible: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

  If another bridge in the same spanning-tree domain does not run the MAC address reduction feature, it could win root bridge ownership because of the finer granularity in the selection of its bridge ID.

- Cisco IOS software Release 12.2SX does not support:
  - Integrated routing and bridging (IRB)
  - Concurrent routing and bridging (CRB)
  - Remote source-route bridging (RSRB)
- Use bridge groups on VLAN interfaces, sometimes called fall-back bridging, to bridge nonrouted protocols. Bridge groups on VLAN interfaces are supported in software on the MSFC.
- Cisco IOS software Release 12.2SX does not support the IEEE bridging protocol for bridge groups. Configure bridge groups to use the VLAN-bridge or the DEC spanning-tree protocol.
- FlexWAN module interfaces support dNBAR. Do not configure NBAR or dNBAR on other interfaces.
- Ingress IP Packets with TTL=1 that are not addressed to the MSFC and that match QoS filtering parameters might cause overpolicing of other ingress traffic on the same ingress interface.
- When the outgoing interface list for group G traffic transitions to null on a last-hop multicast router, the router sends a (*,G) prune message to the PIM neighbor toward the rendezvous point (RP) to stop the flow of group G traffic (if any) down the shared tree, but does not send an (S,G) prune message to stop the flow of traffic down the shortest path tree (SPT). The transition of the outgoing interface list to null does not trigger an (S,G) prune message. (S,G) prune messages are triggered by the arrival of (S,G) traffic.

  If the last-hop multicast router is a Catalyst 6500 series switch, traffic is forwarded in hardware. In most cases, RPF-MFD is installed for the (S,G) entries. The MSFC does not see the multicast traffic flowing down the SPT and does not send any traffic-triggered (S,G) prunes to stop the flow of traffic down the SPT. This situation does not have any adverse effect on the MSFC because the PFC processes and drops the unwanted (S,G) traffic.
- Cisco IOS software Release 12.2SX does not support network booting.
- The IP HTTP server feature is disabled by default. Enter the **ip http server** command to use the feature.
- For LAN switching modules, the Cisco IOS **show controllers** command generates no output in Cisco IOS software Release 12.2SX. Enter the **show module** command instead.
- To avoid the case where all traffic is out of profile, the burst size specified in a QoS policing rule must be at least as large as the maximum packet size permissible in the traffic to which the rule is applied.
- By default, the MSFC sends Internet Control Message Protocol (ICMP) unreachable messages when a packet is denied by an access group.

  With the **ip unreachables** command enabled (which is the default), the supervisor engine drops most of the denied packets in hardware and sends only a small number of packets (10 packets per second, maximum) to the MSFC to be dropped, which generates ICMP-unreachable messages.

  To eliminate the load imposed on the MSFC CPU by the task of dropping denied packets and generating ICMP-unreachable messages, you can enter the **no ip unreachables** interface configuration command to disable ICMP unreachable messages, which allows all access-group denied packets to be dropped in hardware.
- MAC address-based Cisco IOS ACLs are not supported for packets that are Layer 3 switched in hardware. MAC address-based Cisco IOS ACLs will be applied on software-switched packets.
- If you enable multicast routing globally, then you should also enable multicast routing (using the **ip pim** command) on all Layer 3 interfaces on which you anticipate receiving IP multicast traffic. This command causes the packets to be sent to the process switching level to create the route entry. If you disable multicast routing on the RPF interface, the entry cannot be created and the packet is dropped.

If the source traffic rate exceeds what can be handled by the process level, it can have an undesirable impact on the system. For example, routing protocol packets, such as EIGRP hello packets, might get dropped.

- The in and out ports displayed in Layer 3 table entries are set by the hardware at the time the entry is created. They are not guaranteed to be accurate in case multiple flows use the same entry (for example, if the flow mask is **Dest-only** and some kind of load sharing is active) or if the source or destination of the Layer 3 entry moves in the Layer 2 topology. The port information is not always available when the Layer 3 entry is established. This is the case if the destination port of the rewritten packet is unknown when the shortcut is created.
- For EtherChannels, you can configure the QoS trust state and default CoS directly on the EtherChannel interface with the **mls qos trust** or **mls qos cos** commands, respectively. These two parameters must be the same for all physical interfaces in the channel. No other QoS queueing configuration commands can be applied to EtherChannel interfaces. Other QoS queueing configuration commands can be applied, however, to individual EtherChannel physical interfaces. After the physical interfaces are bundled into an EtherChannel, QoS classification, marking, and policing by the Policy Feature Card (PFC) for the channel packets is determined by the service-policy attached to the EtherChannel interface. The service policies attached to the individual physical interfaces of the EtherChannel do not matter. The same is true for the port-based and VLAN-based QoS state of the EtherChannel interface. You can disable the PFC QoS features using the **no mls qos** interface configuration command on the EtherChannel interface.
- The maximum recommended number of Layer 3 multicast entries is 10,000. The maximum recommended number of multicast entries supported in the Layer 2 forwarding table is 12,000.
- After enabling Protocol Independent Multicast (PIM) on an interface, you need to enter the **ip mroute-cache** command on the interface to enable multicast fast-switching. If you have “no ip mroute-cache” configured, multicast packets that are not hardware switched will go to the process level that increases the load on the router.
- FlexWAN ports do not support SPAN or RSPAN.
- MPLS on the FlexWAN module does not support Virtual Private LAN Service (VPLS).

# Caveats


- Caveats in Release 12.2(33)SXJ and Rebuilds, page 213
- Caveats in Release 12.2(33)SXI and Rebuilds, page 251
- Caveats in Release 12.2(33)SXH and Rebuilds, page 369


## Caveats in Release 12.2(33)SXJ and Rebuilds


- Caveats Open in Release 12.2(33)SXJ and Rebuilds, page 213
- Caveats Resolved in Release 12.2(33)SXJ6, page 215
- Caveats Resolved in Release 12.2(33)SXJ5, page 216
- Caveats Resolved in Release 12.2(33)SXJ4, page 218
- Caveats Resolved in Release 12.2(33)SXJ3, page 221
- Caveats Resolved in Release 12.2(33)SXJ2, page 223
- Caveats Resolved in Release 12.2(33)SXJ1, page 229
- Caveats Resolved in Release 12.2(33)SXJ, page 234


### Caveats Open in Release 12.2(33)SXJ and Rebuilds

| Identifier | Component | Description |
|---|---|---|
| CSCsx31739 | bgp | Outbound policy changes does not reflect by itself in MTR Code base |
| CSCsy27228 | bgp | Eagle_cnh: Match statement fail to match prefixes |
| CSCsz28538 | c3pl | SPA Timeout for All SPA's on Boot-up. |
| CSCtn39432 | c6k-es40 | SVI EoMPLS and VPLS not working on ES40 |
| CSCta03464 | c6k-sip-400 | VPLS VC hardware entry lost upon reroute and TE FRR tunnel shutdown |
| CSCtq20866 | c6k-wan-common | Memory leak observed @ c6k_atom_msg on sp after removing xconnect |
| CSCtz22632 | c6k-wan-common | sxj3: Logs are seen when interface is suppressed |
| CSCtq64944 | cat6000-acl | c2wa1b: TCAM not program'd when new DHCP address received |
| CSCtz17231 | cat6000-acl | Bulk-sync failure due to PRC mismatch when ACL is config with portgroup |
| CSCsz70263 | cat6000-cfm | CFM on ISL links isn't working correctly. |
| CSCtt36279 | cat6000-diag | NAM-3: CONST_DIAG-SW2_SPSTBY-3-HM_TEST_FAIL during OIR |
| CSCtu01395 | cat6000-diag | c2wa1c: ASA in switch 2 resets twice on OIR |
| CSCtq56225 | cat6000-dot1x | Multiple Authorized types seen for dot1x supplicants |
| CSCue59987 | cat6000-energywise | Input queue size becomes negative with energywise enabled. |
| CSCsy24099 | cat6000-ha | get platform-provided x-matrix table on RP |
| CSCtl42874 | cat6000-l2-ec | C2WA1 : mLACP : "mlacp min-link" errdisable upon backbone intf fail/recv |
| CSCtu92977 | cat6000-l2-ec | LACP Po is retaining hash algorithm command even after removal of PO |
| CSCsm59426 | cat6000-l2-infra | UDE/UDLR: OSPF neighbourship is not getting formed with UDE/UDLR link |

| Identifier | Component | Description |
|---|---|---|
| CSCtq06060 | cat6000-lacp | LACP config re-appeares after PO detele/recreate sequence |
| CSCsx08647 | cat6000-ltl | Traceback at  bitlist_validbit within vs_ltl_mgr_proc |
| CSCsu66341 | cat6000-mcast | W2: 'MLS MSC' ISSU client needs error buginf, for incompatible case |
| CSCtj66981 | cat6000-mcast | MET2 is not programmed for new SR translation rules added in ISSU RV |
| CSCsu68054 | cat6000-netflow | Cat6k Platform changes required for BGP  4-bytes AS Numbering |
| CSCsx76244 | cat6000-portsecur | Sup720-Standby continuously reboots on psec mac-move violation with prot |
| CSCsv53086 | cat6000-routing | ipv6 traffic route-cache switched at ipv6ip tunnel (over mpls)c tail end |
| CSCsw70162 | cat6000-span | C2W21: Span port capture duplicated port-channel packets after SSO |
| CSCtl82303 | cat6000-svc | c2wa1: Stdby switch crashes @l2_maclimit_update_src_index_change |
| CSCtq28029 | cat6000-svc | VSS: hw-mod mod <ASASM mod#> reset doesn't work Gives invalid error |
| CSCtr30113 | cat6000-svc | Standby reloads and never comes up after SSO in the VSS with fwsm |
| CSCts84327 | cat6000-svc | IDSM/NAM will not come up when power off followed by power on |
| CSCtt28763 | cat6000-svc | NAM-3: command hw-module reset doesn't work at certain condition |
| CSCtu00733 | cat6000-svc | NAM3 got pwrDown by hw-module module reset cmd |
| CSCsw50021 | cat6k-vs-proto | After SSO, FIBIDBINCONS1: An internal software error occurred |
| CSCtn76064 | debug | ACE 30 and ACE 20 reboots in SSO redundency |
| CSCtb95854 | ha-ifindex-sync | %IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex, on LV & RV |
| CSCte71854 | itasca-scp | ACE 30 and ACE 20 reboots in SSO redundency |
| CSCtz12715 | nat | TB while deleting Static nat entry which has interface as global address |
| CSCty94040 | nat-pat | Nat46 traffic through Arsenal ASA does not flow without ipv6 SVI |
| CSCsr93564 | pem | AUTHZ success with wrong DACL entry. |
| CSCsy47965 | pem | FID:for non existent fid ACL on the switch, authz is success |
| CSCts05237 | pem | "sh epm sess inter <x/y>" dispplays all existing epm sessions |
| CSCty32463 | pki | Kingpin & 1RU Unable to sync  in SSO mode w/ 'crypto pki' configuration. |
| CSCtz20394 | socket | Invalid TCB pointer TBs seen on NAM process upon clearing tcp sessions |
| CSCsz29842 | tcp | %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x9BFAC6C0 -Process="RSMP Server |
| CSCtn12371 | vpn-sm | SPA-IPSEC-2GE: XDR-6-XDRLCDISABLEREQUEST  / Traceback |
| CSCtn77107 | wlc-kernel | WiSM-2 Data port Down on VSS after multiple SSO or stdby switch reset |
| CSCts96124 | wlc-os | Sessioning to Jian not happening after changing service vlan subnet |

# Caveats Resolved in Release 12.2(33)SXJ6

### Resolved gsr-boot Caveats

- CSCsv74508—Resolved in 12.2(33)SXJ6

  **Symptom:** If a linecard is reset (either due to error or a command such as **hw-module slot reload**) at the precise time an SNMP query is trying to communicate with that LC, the RP could reset due to a CPU vector 400 error.

  **Conditions:** In order to experience these symptoms the linecard is reset (either due to error or a command such as **hw-module slot reload**) at the precise time an SNMP query is received.

  **Workaround:** None

  More Info: None.

### Resolved ios-authproxy Caveats

- CSCtz99447—Resolved in 12.2(33)SXJ6

  **Symptom:** Local webauth and HTTP services stop responding on the switch.

  **Conditions:** A **show processes | inc HTTP Proxy** command lists many instances of the HTTP Proxy service, and these do not disappear.

  **Workaround:** The HTTP Proxy service may experience delay due to an incorrectly terminated HTTP or TCP session. In some cases, increasing the value of **ip admission max-login-attempts** works around this issue. In others, the stuck HTTP Proxy service will again become available after a TCP timeout.

  Some browsers and background processes using HTTP transport can create incorrectly terminated HTTP/TCP sessions. If webauth clients are under control, changing web browsers or eliminating background processes that use HTTP transport may eliminate triggers for this issue.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

  CVE ID CVE-2012-4658 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

| Identifier | Component | Description |
|---|---|---|
| CSCub04965 | aaa | TCP Session hung causing Packet loss |
| CSCug62154 | aaa | Mk1: High CPU 100% due to TPLUS with tacacs config |
| CSCuh43252 | aaa | unable to login and high cpu when authenticating with TACACS |
| CSCsl04415 | bgp | 1000 ipv6 ebgp sessions does not come up on 6vpe , only 300 come up |
| CSCud08574 | c6k-crypto | Vlan Interface over Serial - IPCP nego and Vlan link-up race condition |
| CSCsu63884 | c7600-netflow | 7600 netflow: workaround to scale RP sampled flow export per PD ratio |
| CSCug23641 | cat6000-acl | FM missing dot1x feature for interface; IPDT entries & dACLs failing. |
| CSCub23671 | cat6000-dot1x | Authentication loop in dot1x->mab->guest vlan for supplicantless PC |
| CSCub60449 | cat6000-dot1x | Switch starts second authentication after port in guest vlan |
| CSCud22789 | cat6000-dot1x | IGMP joins when port is in auth-fail state not forward to mrouter |

| Identifier | Component | Description |
|---|---|---|
| CSCue31621 | cat6000-dot1x | MAB fails after 6500 reload when port configured for critical voice vlan |
| CSCue02511 | cat6000-fabric | VSS FPOE incorrect on standby |
| CSCue53095 | cat6000-firmware | ISSU fails between SXI and SXJ on Sup32/S720-10G for certain versions |
| CSCua87594 | cat6000-l2 | cat6k:Spanning Tree interop between MST0 & RSTP takes 6 secs to converge |
| CSCtu01035 | cat6000-l2-infra | OIR heathland module on newly active during standby bootup crash both |
| CSCuf36123 | cat6000-l2-infra | VSS Standby crash after renaming vlan |
| CSCtw49851 | cat6000-mcast | show ipv6 mld snooping explicit-tracking cli o/p changed |
| CSCue52637 | cat6000-mcast | Multicast traffic blackholed after deleting a vlan |
| CSCuh41546 | cat6000-qos | Standby is getting crashed after ISSU Runversion |
| CSCud18108 | cat6000-snmp | CAT6500 SNMP timeouts polling dot1dTpFdbTable |
| CSCue03531 | cat6000-snmp | 6500-Transceiver/SFP SNMP polling interrupted when changing port config |
| CSCua01409 | cat6000-svc | C4Ma2:TB and Standby reload on adding & removing fwsm config |
| CSCtg57657 | dhcp | Router crash at dhcp function |
| CSCub75883 | ip-acl | Access-line numbers are NOT persistant after reload |
| CSCui17285 | ip-acl | ip access-list persistent keyword not available in SXJ6 image |
| CSCee38267 | nat | NAT router may reload under heavy load of NAT traffic |
| CSCtx95334 | nat | TCAM entries are not correctly programmed for static nat w/ interface |
| CSCue21223 | nat | Intermitant HSRP hellos not sent w/ IP NAT redundancy configured on SVI |
| CSCsc97279 | nvram | Takes long time (more than 2 minutes) on wr mem |
| CSCud65003 | parser | router crash during config of priv level exec commands |
| CSCsw43080 | rsr-bridging | Traceback seen @ data_inconsistency_error_with_original_ra |
| CSCtd45679 | sla | Removing ip sla probe (configured by SNMP) in CLI reloads Standby Sup |
| CSCue80816 | snmp | Crash while routine config push through SNMP |
| CSCsd72758 | ssh | Scheduler Thrashing in the SSH Process |
| CSCud79481 | udp | Crash on 6500 on executing "show ip helper address" |

## Caveats Resolved in Release 12.2(33)SXJ5

### Resolved nat Caveats

- CSCtg47129—Resolved in 12.2(33)SXI11

  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:**

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

**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:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

### Resolved Cisco IOS Caveats

- CSCua63614—Resolved in 12.2(33)SXJ5

  **Symptom:** When Energywise is enabled on Cat6500 switch, input queue drops can be seen on the interfaces connected to other Energywise neighbors

  **Conditions:** EnergyWise is enabled on Cat6500 and on connected device

  **Workaround:** None

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.3/2.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Other Resolved Caveats in Release 12.2(33)SXJ5

| Identifier | Technology | Description |
|---|---|---|
| CSCtg48829 | — | Memory leak at set_dst_card_ports+ |
| CSCth11657 | — | switch reboots during taking core file with standby sup. Simplex ok |
| CSCtx50235 | — | SP and RP mutually resetting each other hides the actual crash reason |
| CSCty15494 | — | Memory leak in cfib_fibsb_chunk |
| CSCtz36880 | — | SXJ3: ACE30 IPv6 RHI throws TB |
| CSCtz52826 | — | SXJ1 VSS crash on redundancy force-switchover |
| CSCua08468 | — | SG Entries installed as Partial-SCs and do not switch to Data MDT |
| CSCua43298 | — | Port loopback mode may not be cleared in corner case |
| CSCub07847 | — | High CPU seen on receiving DHCPINFORM on SVI with pbr enabled |
| CSCub29359 | — | ISSU from SXI to SXJ on VSS resets with WS-SVC-WISM2-K9 installed |
| CSCub38767 | — | Devices connected to WS-X6148E-GE-45AT are unable to ping SVI |
| CSCub52879 | — | CCP loopback test for Jian fails upon removal of service-vlan config |
| CSCub63550 | — | CDP fails when crypto connect is configured on a SPA-2x1GE inteface |
| CSCub72971 | — | inrerface resets counter shows 4294967295 after module OIR/switchover |
| CSCub94085 | — | SXJ: CSM/CSM-S/SSLM modules should be powered down |
| CSCub94186 | — | MPLS TE FRR with auto-bandwidth causes hw adj leak/glean on recalc |
| CSCuc45901 | — | VSS IPv6 RHI route from ACE doesn't get removed |

| Identifier | Technology | Description |
|---|---|---|
| CSCuc50707 | — | Crash in idbman_if_clear_vlan_id when doing default switchport |
| CSCuc65082 | — | monitor capture view/privilege setting causes MALLOC failures |
| CSCuc98078 | — | Basic Multi-host mode authorization is broken |
| CSCud15384 | — | Vlan-Based Qos fails for Wism module |
| CSCud83152 | — | MVPN traffic punted to RP due to misprogrammed MTU |
| CSCts87275 | Infrastructure | Cat4k with sup7e : same snmp engineID on different cat4k switches |
| CSCty04899 | Infrastructure | 6500 - Smart Call Home ignores custom http port configuration |
| CSCtz74540 | Infrastructure | 2 Sup VSS - Mistral interrupt on SP : old active remains in RP Rommon |
| CSCua70136 | IPServices | NAT VRF with PAT - PPTP translation failure with dynamic pool |
| CSCub18395 | IPServices | PAT not working when shut/no shut nat+hrsp config interface |
| CSCub65395 | IPServices | Sup720 crashes at dhcpd_forward_reply |
| CSCub78079 | IPServices | NAT per VRF: parser fail with route-map applied to static nat |
| CSCud08682 | IPServices | NAT not translating Traceroute's ICMP Unreachables |
| CSCud09626 | IPServices | NAT PPTP use_count 1 entry not removed if TCP data segment with FIN flag |
| CSCud51025 | IPServices | DHCP relay crash @dhcpd_relay_remove_info_option |
| CSCud89194 | IPServices | Backout fix for CSCub22017 for sxj |
| CSCud95251 | IPServices | static nat with vrf looses vrf name after nat translations expire |
| CSCtd54694 | Management | Switch crashes on Show cdp neighbor detail in some conditions |
| CSCua66870 | Multicast | PIM-Dense: OIF on (*,G) is pruned due to RPF changed on (S,G) |
| CSCub09124 | Multicast | MVPN MDT failure due to multicat boundary on non-current RPF interface. |
| CSCtk37079 | Routing | Traceback seen @ ip_sendself |
| CSCtq49325 | Routing | EIGRP graceful shutdown can cause a reload |
| CSCtr58140 | Routing | PFR controlled EIGRP route goes into SIA and resets the neighbor |
| CSCtt02313 | Routing | PfR: Uncontrol TC due to Exit Mismatch |
| CSCtx04709 | Routing | Active routes remain in topology but does not go SIA after route lost |
| CSCtz84714 | Routing | IPv6 : snmpwalk on cIpAddressPfxOrigin does not return /64 subnets |
| CSCub21480 | Routing | Crash at bgp_vpn_impq_add_vrfs_importing when removing import ipv4 cmd |
| CSCuc63629 | Routing | ip vrf forwarding on vlan fails whenever vlan interface shut/no shut |

## Caveats Resolved in Release 12.2(33)SXJ4

### Resolved Routing Caveats

- CSCef01541—Resolved in 12.2(33)SXJ4

  A router processes a packet that is sent to the network address of an interface, if the Layer 2 frame that is encapsulating that packet is specifically crafted to target the Layer 2 adress of the interface or a broadcast Layer 2 address.

  This happens only in the process switching path and does not happen in Cisco  Express Forwarding (CEF) path.

  Workaround is to use CEF.

### Resolved Security Caveats

- CSCtl59829—Resolved in 12.2(33)SXJ4

  **Symptom:** Login success and failure messages only display the first 32 bits of the IPv6 source address in IPv4 format.

  Source Address FC00::1

  *Aug 5 19:39:07.195: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: cisco] [Source: 252.0.0.0] [localport: 23] [Reason: Login Authentication Failed - BadPassword] at 19:39:07 EST Wed Aug 5 2009

  **Conditions:**

  - Telnet or SSH from IPv6 enabled device to IPv6 address on router or switch.
  - Have login success and failure logging enabled.

    ```
    login on-failure log
    login on-success log
    ```

  **Workaround:** None

  **Further Problem Description:** The IPv4 address is derived from the first 32 bits of the IPv6 address.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4/3.3:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:P/A:N/E:F/RL:OF/RC:C

  No CVE ID has been assigned to this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Resolved Cisco IOS Caveats

- CSCtr88193—Resolved in 12.2(33)SXJ4

  **Symptom:** Either High CPU or Crash resulting from large number of ipv6 hosts.

  **Conditions:** This has been seen while sending Multicast Listener Discovery packets with IPv6 and mld snooping enabled.

  **Workaround:** none

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.7/4.7:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-3062 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Other Resolved Caveats in Release 12.2(33)SXJ4

| Identifier | Technology | Description |
|---|---|---|
| CSCta74577 | — | Need to print out module number is message LTL-SP-2-LTL_PARITY_CHECK |

| Identifier | Technology | Description |
|---|---|---|
| CSCtg11421 | — | All egress traffic dropped by SIP-400 + BusConnectivityTest failure |
| CSCtj76176 | — | Port-Channel members go to w state (Up Mstr Not-in-Bndl) after SSO |
| CSCtl58612 | — | Stby Sup resets with "boot bootldr", but file doesn't exist on stby |
| CSCto73878 | — | Intermittent PAT Order-of-Operations problem |
| CSCto95687 | — | Failure to aquire sem (l2_se_get_ps_sem) for a long time leads to crash |
| CSCtr05488 | — | Enhanced FlexWAN (WS-X6582-2PA) silently reload during BERT w/o crashinf |
| CSCtr39973 | — | c2w2: Diag failure after second sso with arp policing |
| CSCtr92285 | — | MPLS L2VC down as no SSM ID allocated to VC |
| CSCts98176 | — | RRI routes missing while IPsec SA is up |
| CSCtt04914 | — | Span stops working and must be re-configured to continue working. |
| CSCtt96152 | — | VSS: corrupted Portchannel: LTL missing VSL-link |
| CSCtw55546 | — | Cat6k:sh lacp internal detail output shows wrong Timeout value |
| CSCtw80411 | — | MAB - Fails for devices already connected when enabled |
| CSCtw81160 | — | Auth session successful even when Filter-ID application fails |
| CSCtw89269 | — | Ports in 2X1GE-V2 SPA is not coming UP with configured speed |
| CSCtx43498 | — | cat6500: Some DACL entries may not be pushed to the switch TCAM |
| CSCty07538 | — | Incorrect static NAT translation leads to TCP reset |
| CSCty20876 | — | Show stack does not show correct Information of Last System Crash - SP |
| CSCty21663 | — | EBGP peer flap with mcast traffic cause cpu spike , ospf and ebgp flap |
| CSCty26260 | — | 6500 - Stndby Sup not fluching mac when port-security is enabled |
| CSCty38102 | — | STP BPDUs not reaching neighbor switches when capture type span cnfged |
| CSCty40181 | — | VSS: L3VPN traffic not forwarded after switchover |
| CSCty94405 | — | DCP and CCP loopback ondemand tests fail without Jian LAG configured |
| CSCty97033 | — | Duplex not changing using snmpset |
| CSCty97492 | — | Not all ARP queries going out when port-channel (DEC) is brought back up |
| CSCtz02829 | — | IDSM: some config not getting sync'd to standby properly |
| CSCtz12050 | — | Not possible to disable hol-blocking for X6148 |
| CSCtz28302 | — | SXJ3: WiSM LAG creation throws %EC-SW1_SP-5-CANNOT_BUNDLE1 errors |
| CSCtz35247 | — | HM_TEST_FAIL TestMgmtPortsLoopback consecutive failure for ASASM on OIR |
| CSCtz42708 | — | Sup720 Storm control on unused port causes TestUnusedPortLoopback fail |
| CSCua02641 | — | Multicast traffic has second drop during SSO/NSF |
| CSCua32821 | — | Stanby console can be get even without "enable standby console" |
| CSCub21431 | — | SXJ4: Jian 2nd data port not getting bundled to LAG upon reload |
| CSCth83143 | Infrastructure | IPv6 access list applied to SNMP community string does not work |
| CSCti80535 | Infrastructure | "Default interface range command" cause standby SUP reset |
| CSCtk36938 | Infrastructure | %SYS-SP-3-CPUHOG @preemption_forced_suspend |
| CSCtx51515 | Infrastructure | backup config using archive feature, generates two files instead of one |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd17017 | IPServices | New NAT entry in table when serial int flaps, seeing connectivity issues |
| CSCsx28822 | IPServices | Memory leak in the Redundancy inter-device feature (rf task) |
| CSCsz24818 | IPServices | ASR:MCP_DEV- RP crash observed when trying to telnet using v6 address |
| CSCtg41289 | IPServices | DHCP pad option is garbage |
| CSCtr30487 | IPServices | Memory Leak with static nat - NAT String Chu |
| CSCtz85702 | IPServices | NAT TCP pptp-control timing-out use_count 1 - entry not removed |
| CSCua43193 | IPServices | Dynamic NAT'g of TCP traffic fails when redudancy VIP is used for NAT |
| CSCtc42278 | ISDN | %DATACORRUPTION-1-DATAINCONSISTENCY - ISDN incoming call |
| CSCtz48619 | MPLS | LDP Typed Wildcard FEC Capability TLV uses wrong value |
| CSCto64160 | QoS | Path tear not sent for all the sessions on "clear ip rsvp senders * " |
| CSCtf13343 | Routing | Authorization and accounting fail for commands including BGP ASNs |
| CSCtf54561 | Routing | Crash in 'show ip cef vrf' with large number of entries |
| CSCtn02656 | Routing | BGP filtering is incomplete after prefix-list reconfiguration |
| CSCto02448 | Routing | Lost of BGP as-path when clearing BGP soft- all become Local routes |
| CSCtz51004 | Routing | VRF route leaking deletes routes on NSF Helper after Switchover |
| CSCtz60771 | Routing | 0.0.0.0/1 BGP prefix wrongly originated causing routing issues |
| CSCty26147 | Security | CIPSO pkt. not getting ignored on tunnel interface running 12.2(33)SXI6 |
| CSCto55708 | WAN | Build Error @ /ip-core-apps/ntp/ntpcore/src/refim/ntp_loopfilter. c:350 |
| CSCto71384 | WAN | 892J Source address is incorrect after source interface is down |
| CSCtt04371 | WAN | Need to change the default setting in NTPv4 for faster sync |
| CSCtw45592 | WAN | CLI "NTP Server <dns name>" - does not get synced to standby |

## Caveats Resolved in Release 12.2(33)SXJ3

### Resolved IPServices Caveats

- CSCts12366—Resolved in 12.2(33)SXJ3

  **Symptoms:** Memory may not properly be freed when malformed SIP packets are received on the NAT interface.

  **Conditions:** None

  **Workaround:** None

  **Further Problem Description:** None.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-2578 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Other Resolved Caveats in Release 12.2(33)SXJ3

| Identifier | Technology | Description |
|---|---|---|
| CSCth40213 | — | multiple pre-shared keys with address 0.0.0.0 not supported |
| CSCth78343 | — | Fetching PSK from keyring should not be restricted to local addr config |
| CSCtj34656 | — | debug ip routing shows non-RIB related events |
| CSCtj40564 | — | crypto keyring binding with local address is broken in some scenarios; |
| CSCtj46927 | — | MF:Access Vlan is removed when 802.1x is enabled on port |
| CSCtl72207 | — | Cat2960: MED information missing in LLDP packets |
| CSCtn05007 | — | ip multicast boundary command not filtering in both directions |
| CSCtn22339 | — | Pre-shared-key lost after router reload |
| CSCtq31974 | — | c2wa1b: multicast SR translation not happening after active sup crashes |
| CSCtq61665 | — | c2wa1b: %BIT-STBY-4-OUTOFRANGE: bit 32767 is not in the expected range |
| CSCts02018 | — | Memory leak in Spanning Tree process on SP |
| CSCts27161 | — | VSS:standby reloads due to parser return error command: duplex full |
| CSCts38007 | — | Query Interval mismatch msg appears on a sw where no querier configs |
| CSCts62391 | — | DTP may prevent VSS from fwding UDLD packets to SP after module reload |
| CSCts66625 | — | VRRP master mac-address with Xtag=0 causing high cpu |
| CSCts82451 | — | switch 6509 crash with Bus Error and cv6_new_hwadj |
| CSCts82932 | — | Incorrect dscp-q mapping on trusted interface |
| CSCts90103 | — | Buffer leak on the RP due to IPC messages resulting in a crash |
| CSCtt23872 | — | QoS queueing commands are rejected after manual OIR of module |
| CSCtt24684 | — | GOLD: Minor Errors Incorrectly Reported on a Trifecta Service Module |
| CSCtt96621 | — | TestDCPLoopback fails on data port 2 with Jian LAG configured |
| CSCtu17483 | — | MF:Switch Crashes due to LLDP process |
| CSCtu22335 | — | On a 6500 after a sup switchover arp inspection fails to forward arp |
| CSCtu36321 | — | CVV: Phone mac gets deleted in MATM on CDP 2nd port up/down for MA mode. |
| CSCtu38265 | — | MA2 : Crash seen with http auth-proxy |
| CSCtu75030 | — | FTP of exception core dump after crash times out |
| CSCtw44733 | — | command "default interface" break the cos map on other interfaces |
| CSCtw50375 | — | NF entry does not get dmac updated after next-hop device sends garp |
| CSCtw61876 | — | IGMPv3 leave results in MCAST packet loss for other receivers |
| CSCtw83085 | — | Parity error message thrown when OIR of T3/E3 SPA in SIP200 |
| CSCtw84639 | — | %BIT-4-OUTOFRANGE: bit 32767 is not in the expected range of 1 to 4096 |
| CSCtw85000 | — | On 7600, 'snmp trap link-status' out of sync on WAN GiGE interface. |
| CSCtw93788 | — | MDA port during reauth goes to error disabled state on SSO. |
| CSCtx12231 | — | Config Sync: Bulk-sync failure due to PRC mismatch in ACL |
| CSCtx15569 | — | SPA-IPSEC-2G crash packet size above 1800 |
| CSCtx78044 | — | 6-8 second delay in forwarding mcast after a rapid join/leave/join |

| Identifier | Technology | Description |
|---|---|---|
| CSCtx79489 | — | Follow-up ddts for CSCts62391 |
| CSCtx92952 | — | SUP crash when issuing show upgrade fpd file ftp/tftp cmd |
| CSCtx99818 | — | ISSU from SXI6 to SXI9  failed |
| CSCth64138 | AAA | CPU high@'AAA ACCT Proc' session remains after user disconnects |
| CSCts80209 | AAA | Cat6k switch crash on "no login block-for" with login quiet-mode |
| CSCta67945 | Infrastructure | ifInOctets incorrect values when requested every second with other OIDs |
| CSCti24577 | Infrastructure | Loading a config with banner command creates config sync issues |
| CSCto06915 | Infrastructure | Sup720 remains in ROMMON after SP crash |
| CSCto70125 | Infrastructure | High CPU due to IPSLA tcpConnect probess due to multiple start attempts |
| CSCtw59648 | Infrastructure | BOOTLDR missing from show version |
| CSCtw85356 | Infrastructure | delay auto reflexed on channel interface without config |
| CSCtx13605 | Infrastructure | Need CSCtb92791 Ported to 6500 code OSPF MD5 key gets modified |
| CSCtx68100 | Infrastructure | Reload reason not displayed correctly on some platforms |
| CSCse99493 | IPServices | Router crash with NAT overload and large number of NAT translations |
| CSCsi11368 | IPServices | DHCP Relay agent should remove the relay-info option, not overwrite |
| CSCtl51688 | IPServices | NAT Error registering with Transport Port Manager - Standby Reload |
| CSCtt70568 | IPServices | PPTP timeout entries are never removed from NAT table. |
| CSCtw61104 | IPServices | DHCPv6 LQ:cmts crash with "Corrupted magic value in in-use chunk" |
| CSCtv97307 | MPLS | MLPS LDP flaps with high Tag Control and IPRM CPU utilization |
| CSCts41032 | Multicast | %SYS-2-NOBLOCK: suspend with blocking disabled  tracebacks. |
| CSCtw48209 | QoS | RSVP trap sent when MPLS-TE RSVP session state change may cause crash |
| CSCtf27303 | Routing | 6PE interop: Cisco router sends MP_UNREACH_NLRI in not negotiated SAFI |
| CSCtn78663 | Routing | Cat6k No ICMP Mask Reply |
| CSCtu79372 | Routing | Cat6500 "clear ip route vrf" delete connected routes from ip vrf receive |
| CSCtw81998 | Routing | BGP is not leaking the routes in to vrf using route-map if rib-failure |
| CSCtx01476 | Routing | Config Sync: Bulk-sync failure due to PRC mismatch in ACL |
| CSCto60047 | Security | Chunk corruption crash on trying to abort "show tech" over SSH |

## Caveats Resolved in Release 12.2(33)SXJ2

### Resolved Infrastructure Caveats

- CSCtr91106—Resolved in 12.2(33)SXJ2

  **Summary:** A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

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

**PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 8.5/7:
https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0384 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Resolved IPServices Caveats

- CSCtr28857—Resolved in 12.2(33)SXJ2

  **Summary:** A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  **Note:** The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0382 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Resolved Cisco IOS Caveats

- CSCtq36327—Resolved in 12.2(33)SXJ2

  **Symptom:** A loop between a dot1x enabled port and another a)dot1x enabled port configured with open authentication or b) non-dot1x port, will create a spanning-tree bpdu storm in the network.

  **Workaround:** Avoid creating a loop.

  **Further Problem Description:** This is a day-1 issue and the fix is available in SXI7, SXJ2 and MA2.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2011-2057 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCtq36336—Resolved in 12.2(33)SXJ2

  **Symptom:** An external loop between 2 dot1x enabled ports can cause a storm of unicast EAPoL pdus in the network.

  **Workaround:** Avoid creating a loop.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2011-2058 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCts38429—Resolved in 12.2(33)SXJ2

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

  **Note:** The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

### Other Resolved Caveats in Release 12.2(33)SXJ2

| Identifier | Technology | Description |
|---|---|---|
| CSCek68936 | — | 6716 fabric asic causing EC performance issue |
| CSCsj70829 | — | CPU hog caused by OBFL uptime logging |
| CSCsk94501 | — | AUTHPROXY: info timestamp array size not the same as max-login-attempts |
| CSCsm36855 | — | %MCT1E1-3-TIMEOUT: TB@ cte1_wait_for_linkrec_ready while unconfig chn gr |
| CSCsm43012 | — | Speed value changed during the upgrade automatically from 10M to 100M |
| CSCsr50385 | — | Crash while executing "clear archive" and "show archive" simultaneosly |
| CSCsu06967 | — | auth-proxy-banner must not be displayed on result page |
| CSCtc99947 | — | Switch drops DHCP INFORM packets from DHCP client |
| CSCtg96982 | — | Memleak @ bitlist_chunk_alloc on VSS on standby switch |
| CSCth31231 | — | dACL for MAB still applied for dot1x users |
| CSCth83455 | — | C2WA1b: set default interface <serial interface> is not working |
| CSCti45609 | — | LISP: improve map-cache build-up time |
| CSCtj84234 | — | Packets drop is there when configuring VRF |
| CSCtk00198 | — | Stack master crashed on defaulting ASw interface |
| CSCtl77057 | — | TestErrorCounterMonitor can generate false positive on 67XX cards |

| Identifier | Technology | Description |
|---|---|---|
| CSCtn15098 | — | MF:IDH:Local session timer does not kick in if AAA timer is disabled. |
| CSCtn27420 | — | MF: device tracking causes duplicate address warning on Windows |
| CSCtn78508 | — | vlan range 1002-1005 automatically added to "sw cap allow vlan" command |
| CSCtn81945 | — | MVPN extranet corrupted linkage |
| CSCto53119 | — | ES40:EoMPLS for a vlan X not progmd on LC after allowing&removing frm VE |
| CSCto53223 | — | VSPA\>WS-IPSEC-3 : Failure in VRF Mode acting as EzVPN Server |
| CSCto90846 | — | Tunnel I/F and Vlan I/F stucked on output and dropped packets on Cat6k. |
| CSCto99774 | — | Crash in vtp mib |
| CSCtq21616 | — | Add a cli to line cards to allow viewing of internal framer errors. |
| CSCtq24526 | — | Memory corruption crash in crypto code |
| CSCtq26766 | — | SUP720-3B crash due to large number of IGMP reports received |
| CSCtq26863 | — | Authentication session information sticks when port shut down |
| CSCtq27016 | — | Qos related Memory leak is observed on ES-40 |
| CSCtq34985 | — | DCI: A-VPLS VCs not synced to standby Sup |
| CSCtq35225 | — | Any new SVIs -> NOT coming up due to RP process SW VLAN RP getting stuck |
| CSCtq38187 | — | "VPLS_NP_CLIENT-4-WARN: Invalid VC Index 0 " msg seen in presence of TE |
| CSCtq38419 | — | SP crash on continuous reload of trifecta module |
| CSCtq40606 | — | Span replication loop after switchover on Service Module |
| CSCtq40780 | — | VSS STBY Trifecta x86 waiting infinitly for reset from LCP |
| CSCtq46279 | — | Standby crashes on authz failure when voice and critical vlan are same |
| CSCtq47971 | — | On SSO, IPC communication failed with SIP400 cards: VSS goes to RPR mode |
| CSCtq48027 | — | MVRP: Traffic is NOT flowing in the netwok with MVRP enabled |
| CSCtq48160 | — | cbQosPoliceCfgRateType not set to 2 (Precent) when configured via CLI |
| CSCtq48386 | — | Authfail->Guest, show cmd is incorrect |
| CSCtq48593 | — | VSS:A-VPLSoGRE:Imposotion is not programmed properly after toggling FL. |
| CSCtq50438 | — | c2wa1b: JIAN ports not detected on SIERRA 0523 Image |
| CSCtq51378 | — | TestIPSecEncrypDecrypPkt  message while reloading VSS or SSO |
| CSCtq53902 | — | A-VPLSoGRE:SIP-400:Ingress WRED drops are seen on POS int |
| CSCtq54944 | — | Minor Error and port down on Failover from SXH2a to SXJ in RPR mode |
| CSCtq56136 | — | Input errors incrementing when interface is shutdown |
| CSCtq61884 | — | DHCP snooping for unicast not working to HSRP DMAC |
| CSCtq64820 | — | 6500 SP crash at cmfi_frr_process_stats_counters |
| CSCtq65338 | — | CDP Bypass allows cisco ip phone to bypass aaa in all host-modes.MUSTFIX |
| CSCtq66013 | — | VSS Active switch crashes if Bennu restarted in ACT & then STDBY switch |
| CSCtq72873 | — | MF: Crash @ eap_auth_fail |
| CSCtq75000 | — | SPA3 card crashes when ACL is configured with Port values |
| CSCtq80246 | — | RPW:SVI goes down after removing and adding back the vlan in VE |

| Identifier | Technology | Description |
|---|---|---|
| CSCtq80394 | — | mroute entry not create for sparse default-MDT group |
| CSCtq86628 | — | Traceback at SSO SCHED-SW2_SP-7-WATCH uninitialized boolean "rf task" |
| CSCtq90605 | — | mlapc dynamic priority rollover causes unexpected state |
| CSCtq90744 | — | SNMP trap is not sent for SVI up/down |
| CSCtq94581 | — | voice domain cannot authc when port-security is enabled (MDA mode) |
| CSCtq95922 | — | ASASM power-cycled 'off (Module not responding to Keep Alive polling)' |
| CSCtq98031 | — | VSS: Trifecta not online in any slot of STDBY after removal during TFTP |
| CSCtr01421 | — | cont standby reset "ip source binding <#> vlan <#> <ip> int fa3/8" if L3 |
| CSCtr03012 | — | On SSO, Mcast RPF-MFD fails only with static join @ RPF i/f |
| CSCtr10155 | — | Crash following defaulting an interface configuration in a port-channel |
| CSCtr13929 | — | Primary member link changing with addition of new member to bundle |
| CSCtr15379 | — | Cat6500 running SXJ1 image tries to boot unsupported ES+ module |
| CSCtr19129 | — | VSS - need to suppress "SIBYTE-SW2_DFC2-3-SB_TX_FIFO_UNDRFL" msgs |
| CSCtr26476 | — | cat6k not always putting the link going to VS sup to FWD via uplinkfast |
| CSCtr46076 | — | crash due to: terminated due to signal SIGBUS, Bus error: MF |
| CSCtr47317 | — | Span replication loop after switchover on Service Module |
| CSCtr50629 | — | Entity Display MIB shows incorrect ACTIVE & POWER MGMT LED status in VSS |
| CSCtr51180 | — | IPSEC-2G in CC on subif reprograms badly icpu vlan map on change |
| CSCtr51517 | — | SSH UNEXPECTED_MSG debugs do not display IP address |
| CSCtr52081 | — | packet storm with external loop on dot1x/mab ports in singlehost mode |
| CSCtr61390 | — | Standby SUP crash @ when its booting with SXI and SXJ image |
| CSCtr67276 | — | PBR within a VRF with object tracking not working on Cat6k |
| CSCtr67722 | — | SP CPUHOG on VSS setup with span session |
| CSCtr68112 | — | SW installed NF entry does not get updated when next-hop sends garp |
| CSCtr73095 | — | LAG data-ports going into Suspended with extend Vlan |
| CSCtr78814 | — | MAJ, GOLD, diag_get_port_group(): module 8 - port group table is NULL |
| CSCtr82360 | — | %EARL_L2_ASIC-DFC4-4-DBUS_HDR_ERR: EARL L2 ASIC #0: Dbus Hdr. |
| CSCtr84253 | — | cat6k rapidly exhausts system buffers |
| CSCts03905 | — | NAM GUI access causes SNMP CPU 100% |
| CSCts09685 | — | %EC-SP-5-CANNOT_BUNDLE2 is logged against the auto-gen EC for WiSM |
| CSCts14723 | — | Non-rpf global timer inconsistency in SXJ1 |
| CSCts15934 | — | VSS: MALLOC failure reported by diag_display_fpoe_entries |
| CSCts19697 | — | VSS:number of inrerface resets shows 4294967295 when switchover |
| CSCts24348 | — | PBR "set vrf" causes destination ARPing for punted packets and drops |
| CSCts26267 | — | Standby VSS switch reloads due to parser return error |
| CSCts33952 | — | rsh command fails from within TclScript |
| CSCts49137 | — | show tech redirect command fails in SXJ1 |

| Identifier | Technology | Description |
|---|---|---|
| CSCts49769 | — | CVV: crash @ auth_mgr_ctx_destroy when unconfiguring CVV |
| CSCts55199 | — | A-VPLS with ECMP paths:L2 Multicast traffic is affected for few flows |
| CSCts57516 | — | EzVPN server disconnects all PATed clients |
| CSCts63619 | — | Report REQ_MOD_RESET_ECC2 while R2D2 detect Rx/Tx memory ECC2 error |
| CSCts66142 | — | Reconfiguring "mls ip multicast stub" config does not program tcam |
| CSCts88817 | — | ASA-SM and SVC-NAM3 lock up triggering module reload by switch |
| CSCtt00490 | — | snmpwalk for a N/A DOM-value is returning a bogus value |
| CSCtt16732 | — | SP memory display in wrong on SUP720-3B when running 12.2(33)SXJ1 |
| CSCtt17210 | — | On setting crcSrcERSpanLoVlanMask to zero, device goes for a reset. |
| CSCtt18651 | — | cat6000-qos and Traceback after a no shut of a port  system crash |
| CSCtt26784 | — | SUP32 crashes on power cycle "registration timer event"at 12.2(33)SXI6 |
| CSCtt27865 | — | VSS:A-VPLS:Traffic loss observed for 4 seconds with GRE tunnel |
| CSCtt30593 | — | C6504-E 12.2(33)SXI5 Long ACL cannot setup by Netconf |
| CSCtt35853 | — | Trifecta:VSS - Console Hung Indefinitely at SSO |
| CSCtt38735 | — | SVIs stuck in Administratively Down state, 'no shut' takes no effect |
| CSCtt41811 | — | Disable Support for VSE card in Warren1.Clix Throttle image |
| CSCtt46982 | — | WiSM-2 in switch-1 of VSS loosing native vlan config after reload |
| CSCtu01427 | — | IPSEC-2G in CC on subif reprograms badly icpu vlan map on change |
| CSCtu23938 | — | Device crash @ qos toggling with portchannel config |
| CSCtu28383 | — | Protocol peer down and cannot ping upstream router with load-defer conf. |
| CSCtu50683 | — | Resetting PS on Standby VSS, reduces power from PS on Active VSS member. |
| CSCsd46369 | AAA | IP source address on packets to TACACS server is wrong |
| CSCee38838 | Infrastructure | kadis timer abort reloads router |
| CSCtb89424 | Infrastructure | Crash at saaEventProcessor |
| CSCtq46758 | Infrastructure | process_reschedule_test should not reschedule with mempool_locks_held |
| CSCtq68778 | Infrastructure | After ISSU complete,  the reload reason line in "sh version" is missing |
| CSCsb70368 | IPServices | Bus error at ipnat_delete_entry with PPTP-TCP entry deletion |
| CSCsr17315 | IPServices | Autoinstall process not correct with BOOTP or DHCP server in same LAN |
| CSCtn07696 | IPServices | 6506-E/Sup720 crash related to SYS-3-URLWRITEFAIL: and TCP-2-INVALIDTCB |
| CSCtq14817 | IPServices | Traceback seen @ ipnat_pptp_client_inside |
| CSCtq41121 | IPServices | IOS NAT: unable to reconfigure static nat ports after removal |
| CSCtr16396 | IPServices | TAC+ Code Incorrectly Implements timeout for tacacs-server timeout |
| CSCts00341 | IPServices | CLI requiring DNS lookup cannot be configured when in SSO mode |
| CSCtt02390 | IPServices | VSS: TFTP-Server fails after switchover or when one of the switches down |
| CSCtg48785 | LegacyProtocols | sh x25 hunt-group %DATACORRUPTION-1-DATAINCONSISTENCY: copy err |
| CSCtq73473 | Management | MF: Crash when entering the 'show cdp interface' command |
| CSCti32641 | MPLS | LDP ICCP capability TLV (0x0405) - (0x07) Bad TLV Length |

| Identifier | Technology | Description |
|---|---|---|
| CSCtf21128 | Multicast | (S, G) fwd int is NULL while (*, G) is correct |
| CSCtr88242 | Multicast | PIM-SM doesn't trigger Join message when RPF is changed |
| CSCsd39315 | PPP | distributed multilink bundle should never show no frags rcvd |
| CSCsv04412 | PPP | %MCT1E1-3-TIMEOUT while deleting bundle with CHT1E1 SPA |
| CSCtr22007 | QoS | Bus Error crash in MPLS TE LM Process on 7600 |
| CSCej87096 | Routing | Redistribute OSPF command messed up |
| CSCek39299 | Routing | BGP-NSR:stby keep reset after bulk sync for bgp dampening CLI |
| CSCsg83966 | Routing | Import MAP:sh ip bgp vpnv4 vrf does not show all entities |
| CSCsw63003 | Routing | Continous BGP activity may result in increasing amounts of memory held |
| CSCtn96521 | Routing | When the Spoke (dynamic) peer-group is configured before the iBGP (stati |
| CSCto84723 | Routing | Cat6K Crash when removing ACL with Object Tracking alsol ACE with OG |
| CSCtq43285 | Routing | Routing churn BGP-EIGRP in VRF-Lite |
| CSCtq62273 | Routing | Configuring IPV6 crashes the router. |
| CSCtr58203 | Routing | Upgrade from 12.2(33)SXH5 to 12.2(33)SXI6 ip local policy w/ VRF |
| CSCtr86436 | Routing | Router doesn't respond to ICMP echo-req from vrf to global loopback |
| CSCts16133 | Routing | Sup720 may crash after rebuilding object-group configuration |
| CSCts43881 | Routing | Unexpected RIP route leak/redistribution |
| CSCts68630 | Routing | IPV6 ACLs  doesn't match the traffic as configured |
| CSCsr96084 | Security | %SYS-6-STACKLOW: Stack for process NHRP running low, 0/6000 |

## Caveats Resolved in Release 12.2(33)SXJ1

### Resolved Infrastructure Caveats

- CSCte01606—Resolved in 12.2(33)SXJ1

  **Symptoms:** When Bidirectional Forward Detection (BFD) is enabled, issuing certain CLI commands that are not premption safe may cause the device to restart. This condition has been seen when issuing commands such as “show mem” or“show mem frag detail”.

  **Conditions:** The issue may occur if BFD is enabled on a device that utilizes Pseudo Preemption to implement this feature. The device must be running an affected software build.

  **Workaround:** Disable BFD

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.4/3.8:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C

  CVE ID CVE-2010-3049 has been assigned to document this issue.

  Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Resolved Cisco IOS Caveats

- CSCtj22354—Resolved in 12.2(33)SXJ1

  **Symptom:** System may crash when receiving LLDPDUs.

  **Conditions:** Incoming LLDPDUs with more than 10 LLDP MA(Management Address) TLVs

  **Workaround:** Disable LLDP MA TLV sending on the peers.

  **Further Problem Description:** Currently LLDP supports 10 MA TLVs per LLDP neighbor entry, however, it is not processed properly when more than 10 MA TLVs are received.

- CSCtn76183—Resolved in 12.2(33)SXJ1

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

  **Note:** The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes 9 Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. 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 September 2012 bundled publication.

  Individual publication links are in the "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

### Other Resolved Caveats in Release 12.2(33)SXJ1

| Identifier | Technology | Description |
|---|---|---|
| CSCsr28710 | — | SIP200_MP-4-PAUSE CPUHOG during SIP-200 OIR. |
| CSCsr95189 | — | VSS standby switch reset parser error in IDSM config command |
| CSCsu65095 | — | switch crash w traceback after applying "eou rev all" |
| CSCsu65401 | — | tclsh does not send username to AAA server for command authorization |
| CSCsv60305 | — | DMVPN: Missing listen crypto socket when tunnel interface is up |
| CSCsw89720 | — | CPU-HOG error messages are seen when we query cbQosPoliceStatsTable. |
| CSCsz72735 | — | VSS STP state change over port channel |
| CSCtc06629 | — | crash/tracebacks seen @ crypto_ident_count_ipsec_sas_to_peer |
| CSCtd58259 | — | sw voice vlan - port removed from STP if snmpset commands are executed |
| CSCtd70009 | — | IPphone second port notification not clearing session on 2k |
| CSCtd74965 | — | DSCP marking on VTP packets needs to be changed |
| CSCte95228 | — | ES+ combo keeps reloading after cable OIR |
| CSCtf17152 | — | C2W2C: LACP Auto Interleave HA issue |
| CSCtg09619 | — | Web Auth host gets dropped after DHCP renewal with DHCP snooping enabled |

| Identifier | Technology | Description |
|---|---|---|
| CSCti14287 | — | Unable to display Jian-L CCP and GoreTex SPROM data using show idprom |
| CSCti23324 | — | Remove recirculation for L2 DEC when all ports on ABA cards or later |
| CSCti28450 | — | Show auth session port...and oid returns different results |
| CSCti33299 | — | RP crash due to TLB exception following crypto-map configuration |
| CSCti92970 | — | MF: WoL not working in Multi-Auth |
| CSCtj41144 | — | Tracebacks seen with MLACP config SM-SP-4-BADEVENT: Event 'ct_expired' |
| CSCtj44456 | — | CSM redundancy sync via CLI causes Standby SUP crash if ANM used |
| CSCtj60028 | — | %MGMTINFRA-3-EICORE:Request droped and OOM-0-HIT_MEMORY_THRESH msg seen |
| CSCtj60836 | — | Traceback @ lacp_sm_post_mux_bundle_sync |
| CSCtj76591 | — | WS-X6548-GE-TX:Outdiscards is counted on only SPAN dest port |
| CSCtj84500 | — | Cat6500 - Locked semaphore after config change for CSM WS-X6066-SLB |
| CSCtj95352 | — | SUP32 resets with System NMI:**** SP System NMI: reason 0x00000009 |
| CSCtj99724 | — | SXI1: Memory leak in "mls-msc Process" |
| CSCtk18890 | — | Protected tunnel went down after FRR kicked in |
| CSCtk31978 | — | c2wa1: VSS Act (SW2) reloads after ISSU LV and AV if NAM card is in SW1 |
| CSCtk33826 | — | C2WA1: ISSU cycle from sierra->SXI with 256PO not working |
| CSCtk66648 | — | Traceback Spurious memory access pm_get_bcast_supp_discard_counters |
| CSCtk69755 | — | Trace route in mpls TE not working |
| CSCtl03781 | — | ISSU:ONLINE-SW1_SPSTBY-6-INITFAIL: Module 6: Failed to bring up DFC |
| CSCtl05514 | — | IDSM etherchannel fails after SSO |
| CSCtl05684 | — | XAUTH user remains if authenticated by different user during P1 rekey |
| CSCtl13134 | — | "SVCLC SCP communication failed"  observed on SUP during ACE reload |
| CSCtl23179 | — | Incorrect TCAM Programming when new DHCP address received. |
| CSCtl23494 | — | Dot1x not functioning properly with 3rd party ip-phones |
| CSCtl24871 | — | GLBP virtual mac not programmed in tunnel internal vlan |
| CSCtl42871 | — | Show Transceiver Detail Should Show N/A for all fields Instead of 0.00 |
| CSCtl47635 | — | KB lifetime incorrect in "show crypto session detail" |
| CSCtl54046 | — | Standby Sup crashes@dot1x_get_supp_sb with cts dot1x/manual |
| CSCtl55179 | — | CPU HOG in mlacp process on core isolation |
| CSCtl56002 | — | Traceback seen @ "SCP Write Process" |
| CSCtl58697 | — | c2wa1: Swapping WiSM with JIAN fails to bundle JIAN port in LAG |
| CSCtl58831 | — | small buffer leak on WS-X6708-10GE |
| CSCtl70909 | — | c2wa1: Type6 password encryption is not wrking in Aggressive Mode |
| CSCtl71282 | — | Traffic of Promiscous port is not sent when sec VLAN mode is changed |
| CSCtl73660 | — | c2wa1: IP ACL TCAM doesn't get reset after removing ACL filter from MPA |
| CSCtl75972 | — | CPUHOG for "Virtual Exec" seen when removing/adding ACL on VSS |
| CSCtl76154 | — | c2wa1: WiSM-1 controller 2 status o/p not available in standalone setup |

| Identifier | Technology | Description |
|---|---|---|
| CSCtl76189 | — | On inserting JIAN the  SVC ips of all WISMs/JIANs in the system flushed |
| CSCtl76575 | — | C2WA1: ISSU RPR downgrade followed by upgrade fails with mlacp |
| CSCtl79336 | — | Unable to ping ipv6ip tunnel ipv6 whose tunnel dest ip learned thru MPLS |
| CSCtl82493 | — | c2wa1: After stdby switch reset some Jians and WiSM mgmt ip ping fails |
| CSCtl82681 | — | Not able to configure IPV6 when xconnect is present on main interfacex |
| CSCtl83517 | — | C2WA1: ISSU cycle from sierra->SXI with 256PO not working - red_mode |
| CSCtl85689 | — | c2wa1b : SM Internal Po remains down due to QOS attribute mismatch |
| CSCtl85771 | — | Both ports in DHD goes to P state on doing SSO in Standby POA |
| CSCtl87979 | — | Flexwan card crashes on single bit parity error |
| CSCtl88070 | — | IPv6 VRF configuration causes software punt for global uRPF |
| CSCtl98884 | — | Crashes noticed in AAA create user (kron /console buffer got corrupted) |
| CSCtn00835 | — | Traceroute via mpls cloud does not show egress PE in 3C mode |
| CSCtn01848 | — | Switch crash after shutdown dot1x routed port |
| CSCtn03582 | — | TTL Failure rate-limiter not working |
| CSCtn11825 | — | MVRP error disables L3 interface part of 6148A LC when match registerN/A |
| CSCtn12198 | — | Watchdog timeout after enabling NetFlow |
| CSCtn12243 | — | T/b @ icc_send_mcast_request upon bootup |
| CSCtn14939 | — | Crash and Mem Leak under L2 PIM Snooping config after ISSU LoadVer |
| CSCtn16303 | — | The notification was generated incorrectly by ME-C6524GT-8S. |
| CSCtn18962 | — | ospf :s72033-lanbase-mz image missing subsystems |
| CSCtn26516 | — | C2WA1 : mLACP : Can't unconfig the backbone intf in down state after SSO |
| CSCtn27004 | — | PS AC/DC input sensor is not detected |
| CSCtn27447 | — | Existing option 82 not overwritten but additionally created |
| CSCtn41851 | — | c2wa1:IDSM along with sup not reverting back to cross-bar mode from bus |
| CSCtn43662 | — | Slow memory leak at watcher_create_common (TCP, telnet, watched boolean) |
| CSCtn49482 | — | CONFIG_NV_NEED_OVERRUN and config lock after configuring IDS module |
| CSCtn52363 | — | "channel-group" command missing from member link on module reset |
| CSCtn52549 | — | "show interface" and "show interface counter" is different value. |
| CSCtn55070 | — | call-home http hang, should not use printf in backgroud process |
| CSCtn57039 | — | Memory leak in RADIUS and EAP Framework processes with dot1x configs |
| CSCtn60147 | — | 6500 SXI - L2 traffic is policed when CoPP is enabled |
| CSCtn68317 | — | Cat6500/SXI: DHCP snooping removed from vlan on module OIR |
| CSCtn74068 | — | CSCtl71282 Traffic from Promiscous port isn't switched on mode change |
| CSCtn94479 | — | NAM-3 on VSS:can't reverse telnet & TB after system sso |
| CSCtn96481 | — | wrr-queue cos-map can't be configured |
| CSCto05381 | — | AutoQos on WS-X6716-10GE maps cos values 3,4,6,7 to empty Rx queues |
| CSCto33424 | — | After SSO "mls cef error action reset" cli gets added on standby |

| Identifier | Technology | Description |
|---|---|---|
| CSCto34230 | — | RRI: C6K not remove routes when SAs removed by DPD. |
| CSCto35831 | — | LLDP: incorrect PMD value causes incorrect physical media capability |
| CSCto48396 | — | 6500 LLDP Enabled Capabilities not reporting Bridge capabilities |
| CSCto56118 | — | ACL: Adding a duplicate ACE via an object-group is not rejected |
| CSCto59387 | — | NRGYZ:ERROR:Database uninitialized when walking CISCO-ENERGYWISE-MIB |
| CSCto69916 | — | Apply ACL in order of IPv4 then IPV6 disables TCAM screening on int. |
| CSCto82241 | — | Cat 6500 - MVRP getting enabled on the internal FWSM portchannel |
| CSCto98855 | — | Supervisor crashes in VS mode when VSL LC crashes |
| CSCtq06964 | — | Old Phase ID is used when EzVPN client connect with different ID |
| CSCtq09449 | — | CMTS boot failed and PRE4 crashed for OBFL |
| CSCtq26863 | — | Authentication session information sticks when port shut down |
| CSCtq35225 | — | Any new SVIs -> NOT coming up due to RP process SW VLAN RP getting stuck |
| CSCtq38187 | — | "VPLS_NP_CLIENT-4-WARN: Invalid VC Index 0 " msg seen in presence of TE |
| CSCtq38419 | — | SP crash on continuous reload of trifecta module |
| CSCtq40780 | — | VSS STBY Trifecta x86 waiting infinitly for reset from LCP |
| CSCtq46279 | — | Standby crashes on authz failure when voice and critical vlan are same |
| CSCtq47971 | — | On SSO, IPC communication failed with SIP400 cards: VSS goes to RPR mode |
| CSCtq48027 | — | MVRP: Traffic is NOT flowing in the netwok with MVRP enabled |
| CSCtq48593 | — | VSS:A-VPLSoGRE:Imposotion is not programmed properly after toggling FL. |
| CSCtq50438 | — | c2wa1b: JIAN ports not detected on SIERRA 0523 Image |
| CSCtq53902 | — | A-VPLSoGRE:SIP-400:Ingress WRED drops are seen on POS int |
| CSCtq66013 | — | VSS Active switch crashes if Bennu restarted in ACT & then STDBY switch |
| CSCtq66622 | — | Trifecta Bennu and NAM3 not powered up in Warren1.Bubb throttle image |
| CSCtq75000 | — | SPA3 card crashes when ACL is configured with Port values |
| CSCtq86628 | — | Traceback at SSO SCHED-SW2_SP-7-WATCH uninitialized boolean "rf task" |
| CSCtq95922 | — | ASASM power-cycled 'off (Module not responding to Keep Alive polling)' |
| CSCsc49958 | AAA | aaa authentication fallback to enable caches previously typed password |
| CSCsi83685 | AAA | AAA fallback to radius causes GET_PASSWORD debug message |
| CSCtd21058 | AAA | dACL attribute parsing failed when 'aaa author' debug turned ON |
| CSCtl54415 | AAA | win11(FIT) - dut crashed after trying to ssh to the dut with no key |
| CSCtl77241 | AAA | MF: webauth login triggers switch crash |
| CSCtn19927 | AAA | radius-server attribute 44 Acct-Session-Id not found due to broken CLI |
| CSCed73951 | Infrastructure | banner login #$(hostname)# doesnt work |
| CSCsw81502 | Infrastructure | SNMP HC Poll issue with configurable timer. |
| CSCta09049 | Infrastructure | memory leak in encrypto proc or Pool Manager |
| CSCtf96250 | Infrastructure | IDBMAN-4-CONFIG_WRITE_FAIL and standby sup crash |
| CSCtn50281 | Infrastructure | SNMPv3 uses wrong mac for snmp engine ID |

| Identifier | Technology | Description |
|---|---|---|
| CSCtn78758 | Infrastructure | Crash on Modular IOS on cat6k |
| CSCsu31853 | IPServices | TIMEWAIT TCP sessions cause buffer usage until session expires |
| CSCsv02395 | IPServices | Telnet hostname /vrf <name> does not work |
| CSCtl21288 | IPServices | NAT: "%Port xx is being used by system" even after the CSCtd16493 fix |
| CSCtl21294 | IPServices | NAT: Port numbers are lost from running cfg if route-map option is used |
| CSCtl74114 | IPServices | NAT: static PAT breaks dynamic PAT if they both use the same IP address |
| CSCtn21561 | IPServices | NAT crash while trying to translate DNS reply from an egress interface |
| CSCtn27504 | IPServices | track CLI removed after the reload |
| CSCtn48455 | IPServices | short TCP connections can fail in tcp_open, even if they should work |
| CSCtq41121 | IPServices | IOS NAT: unable to reconfigure static nat ports after removal |
| CSCto59020 | LAN | stp/vtp config change triggers vtp to prune all vlans from forwarding |
| CSCtk64425 | LegacyProtocols | DLSW Ethernet Redundancy not passing ARP with ip arp inspection enabled |
| CSCtl52345 | LegacyProtocols | C3825 bounces back packets with non-owned MAC strangely |
| CSCtn12726 | Management | 'show cdp neighbor detail' causes phone outage in dot1x environment. |
| CSCto68456 | Management | odr incorrectly installs default route out of an L2 interface. |
| CSCsd39315 | PPP | distributed multilink bundle should never show no frags rcvd |
| CSCsz82587 | QoS | Active crashed on module reset[ES20] with LSM configs |
| CSCej87096 | Routing | Redistribute OSPF command messed up |
| CSCsx27496 | Routing | Rtr Crash when imported path is selected as mpath & src route del in RIB |
| CSCtf51640 | Routing | corrupt debug ip packet detail # output |
| CSCtg74011 | Routing | BGP -IPv6 and IPv4 Capability |
| CSCtk15123 | Routing | BGP updates not sent out with update group |
| CSCtl12492 | Routing | Config sync failure after SSO |
| CSCtn16784 | Routing | VRF static route with global keyword not installed in routing table. |
| CSCtn78957 | Routing | High CPU seen with large IPv6 neighbor table |
| CSCto46716 | Routing | TE tunnel is not added into RIB even its found in forwarding-ad and OSPF |
| CSCtk31401 | Security | Router crashes @ssh2_free_keys when exiting the SSH session from client |
| CSCtn07728 | WAN | ntp_ipv6 subsystem missing in SUP720 Lanbase image |

## Caveats Resolved in Release 12.2(33)SXJ

### Resolved AAA Caveats

- CSCth25634—Resolved in 15.0(1)SY

  **Symptoms:** Password is prompted for twice for authentication.

  **Conditions:** This issue occurs when login authentication has the line password as fallback and RADIUS as primary. For example:

  ```
  aaa authentication login default group radius line
  ```

**Workaround:** Change the login authentication to fall back to the enable password that is configured on the UUT. For example:

```
enable password <keyword>
aaa authentication login default group radius enable
```

**Further Information:** The fix for this bug also fixes an unrelated problem that may allow unauthorized users access to EXEC mode if the "line" authentication method is configured with fallback to the "none" authentication method. In other words, if the following is configured:

```
aaa new-model
aaa authentication login MYMETHOD line none

line con 0
  login authentication MYMETHOD
  password <some password>
```

then users providing the wrong password at the password prompt will be granted access.

This issue was originally introduced by Cisco Bug ID CSCee85053, and fixed in some Cisco IOS releases via Cisco Bug IDs CSCsb26389 ("Failover for aaa authentication method LINE is broken") and CSCsv06823 ("Authentication request doesnt failover to any method after enable"). However, the fix for this problem was not integrated into some Cisco IOS releases and this bug (CSCth25634) takes care of that.

Note that Cisco Bug ID CSCti82605 ("AAA line password failed and access to switch still passed") is a recent bug that was filed once it was determined that the fix for CSCee85053 was still missing from some Cisco IOS releases. CSCti82605 was then made a duplicate of this bug (CSCth25634) since the fix for this bug also fixes CSCti82605.

### Resolved Infrastructure Caveats

- CSCti25339—Resolved in 12.2(33)SXJ

  **Symptoms:** Cisco IOS device may experience a device reload.

  **Conditions:** This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  **Workaround:** There is no workaround.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2010-3050 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Resolved IPServices Caveats

- CSCta98734—Resolved in 12.2(33)SXJ

  **Symptom:** DNS Memory Leak in DNS queries

  **Conditions:** DNS server configured: 'ip dns server'

  This bug can only possibly surface if the "ip dns-server" is configured, and then only when specific malformed datagrams are received on the DNS udp port 53. This specific datagram malfrmation is that the udp length field indicates a zero-length payload. This should never happen during normal DNS operation.

**Workaround:** No Workaround at this time

#### Resolved LegacyProtocols Caveats

- CSCth69364—Resolved in 12.2(33)SXJ

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw.

#### Resolved Routing Caveats

- CSCti33534—Resolved in 12.2(33)SXJ

  **Symptoms:** After launching a flood of random IPv6 router advertisements when an interface is configured with "ipv6 address autoconf", removing the IPv6 configuration on the interface with "no ipv6 address autoconf" may cause a reload. Other system instabilities are also possible during and after the flood of random IPv6 router advertisements.

  **Conditions:** Cisco IOS is configured with "ipv6 address autoconf".

  **Workarounds:** Not using IPv6 auto-configuration may be used as a workaround.

  **Further Information:** Cisco IOS checks for the hop limit field in incoming Neighbour Discovery messages and packets received with a hop limit not equal to 255 are discarded. This means that the flood of ND messages has to come from a host that is directly connected to the Cisco IOS device.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.5:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2010-4671 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

#### Resolved Security Caveats

- CSCth45540—Resolved in 12.2(33)SXJ

  **Symptom:** Device crashes in SSH Process

  **Conditions:** SSH process has to fail to allocate memory for the new connection. This would only occur in extremely low memory conditions.

  **Workaround:** None.

#### Resolved Cisco IOS Caveats

- CSCsc60686—Resolved in 12.2(33)SXJ

  **Symptom:** Failed IKE SAs are created when sending specifically formatted IKE messages.

  Although these IKE SAs can be created with 12.4(4)T, they were also created when tested against the IOS c7200-jk96-mz.CSCsc06695 as well which contained a fix for CSCsc06695.

  After IKE SA's are created by the method, they are never auto-removed.

  **Conditions:** Normal operation.

**Workaround:** “clear crypto isakmp 0” which deletes all of the failed IKE SAs

- CSCth87458—Resolved in 12.2(33)SXJ

  **Symptoms:** Memory leak detected in SSH process during internal testing. Authentication is required in order for a user to cause the memory leak.

  **Conditions:** This was experienced during internal protocol robustness testing.

  **Workaround:** Allow SSH connections only from trusted hosts.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2011-2568 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Other Resolved Caveats in Release 12.2(33)SXJ

| Identifier | Technology | Description |
|---|---|---|
| CSCin99433 | AAA | config sync PRC failure seen with kerberos password command |
| CSCsb46724 | AAA | AAA server group doesnt failover with mismatched keys for login |
| CSCsc49958 | AAA | aaa authentication fallback to enable caches previously typed password |
| CSCsw77313 | AAA | failed authentication with login command changes the logged user |
| CSCtb19166 | AAA | Access-Request with EAP Identity Response should not include State attr. |
| CSCtg40901 | AAA | TACACS single connection crashes @tplus_increase_sock_write_event_count |
| CSCtg58029 | AAA | MF:%UTIL-STBY-3-TREE: Data structure error--attempt to remove an unthr |
| CSCth09686 | AAA | "radius-server retry method reorder" removes the server IP upon failover |
| CSCth52843 | AAA | SSO takes 20 to 40 minutes with aaa system accounting |
| CSCti00011 | AAA | MF: NAD sending previous state attribute in EAP Identity request |
| CSCtn19927 | AAA | radius-server attribute 44 Acct-Session-Id not found due to broken CLI |
| CSCsm26150 | ATM | WR-CEOP-SPA: Router crashes @atm_match_vc_group |
| CSCti10891 | ATM | 6500 crash due to ATM following upgrade to SXI4 |
| CSCdx30874 | Cisco IOS | show cry eng conn active shows incorrect interface name on GRE ints |
| CSCed01286 | Cisco IOS | Traceback at em_unlock_internal |
| CSCef71929 | Cisco IOS | DMVPN: HUB displays TED message when TED is not configured. |
| CSCek52883 | Cisco IOS | without IC new peers are added to dyn map instance |
| CSCin99139 | Cisco IOS | oakley_begin_qm seen during XAUTH |
| CSCsb02158 | Cisco IOS | RSA-SIG without CA not working with usage-keys on 2811 |
| CSCsb58856 | Cisco IOS | dialer interface does not kick off interface is cef or fast switchin |
| CSCsb59455 | Cisco IOS | Wrong NAS-Port-Id in Radius accounting |
| CSCsb79586 | Cisco IOS | ISR: eToken removal timeout does not work after hostname change |
| CSCsb94509 | Cisco IOS | With 50 ACLS configured on server ezvpn client connection fails |

| Identifier | Technology | Description |
|---|---|---|
| CSCse29460 | Cisco IOS | distribute-list route-map match source-protocol not working for ospf |
| CSCsg03916 | Cisco IOS | tacacs sys_acct system stop and start not sent after reload |
| CSCsg49757 | Cisco IOS | Combining Gig-Sub-intf & crypto connect & vlan with crypto engine |
| CSCsg78501 | Cisco IOS | IKE should not delete established tunnel upon RSA key regeneration |
| CSCsg96436 | Cisco IOS | EZVPN router using cumulative missed keepalives instead of consecutive |
| CSCsg97955 | Cisco IOS | Small Buffer Leak in send_nat_keepalive w/ crypto isakmp nat keepalive |
| CSCsh50275 | Cisco IOS | DMVPN-ISAKMP Phase 1 gets attached to wrong ISAKMP profile breaks Phase2 |
| CSCsi57874 | Cisco IOS | ID payload protocol/port should be 0/0 instead of 17/0 in aggressive mod |
| CSCsi83806 | Cisco IOS | High CPU on IP Input on MPLS/VPN PE acting as DMVPN Hub |
| CSCsj19194 | Cisco IOS | SP crashes after %PM-3-INTERNALERROR due to switchport flapping |
| CSCsk28857 | Cisco IOS | Packet drops seen during Stress test after first Re-key |
| CSCsm81529 | Cisco IOS | Editting a crypto profile while a console deletes that same prof reloads |
| CSCsq45161 | Cisco IOS | High CPU usage on Virtual-Exec due to renewal of DHCP Snooping database |
| CSCsr39340 | Cisco IOS | MPLS packets are not sent across tunnel |
| CSCsr57766 | Cisco IOS | clear crypto session local <ipaddr> caused CPU HOG crash |
| CSCsr62489 | Cisco IOS | No mask on LC/SP for directly connected prefixes |
| CSCsu67919 | Cisco IOS | SIP crashes - hqf_cwpa_pak_enqueue_local |
| CSCsu69515 | Cisco IOS | auth_mgr: supplicant-name not correctly displayed |
| CSCsv90904 | Cisco IOS | Cat6k: UDP port 2228 is opened by default |
| CSCsw36363 | Cisco IOS | SUP32 temperature sensor AUX-1 temperature: N/O |
| CSCsx96689 | Cisco IOS | Bulk sync failed for stp with 802.1x/MDA |
| CSCsy08264 | Cisco IOS | ES40 QoS: incorrect error handling after running out of bw profiles |
| CSCsy33145 | Cisco IOS | ES+ intf default queues need to be limited to 1% of intf bw on port cong |
| CSCsz72735 | Cisco IOS | VSS STP state change over port channel |
| CSCta24271 | Cisco IOS | 6500 removes switchport access vlan after a dot1x authentication |
| CSCta35728 | Cisco IOS | IPSec deletes wrong tunnel when peer has address change |
| CSCta86571 | Cisco IOS | c4hd1: BIT-SW2_SP-4-OUTOFRANGE TB seen during SS0 |
| CSCtb05389 | Cisco IOS | Alignment errors seen when IKE phase1 failed due to malformed ike packet |
| CSCtc14506 | Cisco IOS | mvpn:PIM neigh over MDT tunnel doesnot come up on del & add vrf on VSS |
| CSCtc32207 | Cisco IOS | Need better accuracy in RP crash reporting |
| CSCtc69463 | Cisco IOS | Interface input rate is doubled the output when BFD is configured |
| CSCtc86019 | Cisco IOS | Infrastructure for VSS SNMP traps transmission |
| CSCtc95709 | Cisco IOS | Called strlen on unitialized (non-null termating) patch digest |
| CSCtd17586 | Cisco IOS | Kron policy cli show tech removed from configuration after occurrence. |
| CSCtd69074 | Cisco IOS | VSS: No resv vlan assigned after del-add VRF after SSO. |
| CSCtd74905 | Cisco IOS | Sup2T-VSL:logging buffered command is not synced with standby after SSO |
| CSCtd84111 | Cisco IOS | IOS SLB doesn't add the CASA input features on an interface |

| Identifier | Technology | Description |
|---|---|---|
| CSCtd91871 | Cisco IOS | EZVPN - memory leak after ungraceful disconnect of client behind PATl |
| CSCte01410 | Cisco IOS | lost packests between FWSM and engine when switchover by SSO |
| CSCte44826 | Cisco IOS | memory leak in cfib_alloc_sb running SXH3a |
| CSCte64898 | Cisco IOS | Vacl capture won't work in Ringar when on different Metro |
| CSCte69094 | Cisco IOS | Hash for the energywise secret changing constantly |
| CSCte71999 | Cisco IOS | Replace ISSU capability negotiation workaround for 4k |
| CSCte75473 | Cisco IOS | SPA-IPSEC-2G is dropping ISIS L2 packets |
| CSCte76841 | Cisco IOS | Adding SP and RP in the middle of crashinfofiles for cat6000 |
| CSCte81219 | Cisco IOS | Inband notification mechanism needed for packet drops due to throttling |
| CSCte90818 | Cisco IOS | MPLS Label to GRE traffic stops on toggling 'mls mpls tun-recir' |
| CSCte95492 | Cisco IOS | C2W2C: Continuous Tracebacks are seen after Second SSO |
| CSCte95819 | Cisco IOS | failover from dot1x to webauth bypassing MAB when dot1x pre-empts MAB |
| CSCte96453 | Cisco IOS | Switch intermittently crashes bringing up port with energywise level 10 |
| CSCte99373 | Cisco IOS | extranet: mrib S,G entry never removed after pim disabled on IIF |
| CSCtf21851 | Cisco IOS | BFD session flap after interface get up status |
| CSCtf23313 | Cisco IOS | C2W2C: Standby Crashes continuously after ISSU LV |
| CSCtf25141 | Cisco IOS | Mem leak seen msc_create_met_set, msc_update_met_set & hal_send_met_job |
| CSCtf28866 | Cisco IOS | Ping and routing protocols go down on VS after RR mode change due to ltl |
| CSCtf33948 | Cisco IOS | PC behind phone authenticates twice. |
| CSCtf49490 | Cisco IOS | dot1x authentication manager inactivity crash upon trunk interface flap |
| CSCtf50155 | Cisco IOS | CDP neighbors aren't seen on layer2 subinterface |
| CSCtf61757 | Cisco IOS | 4sup: Power to module in slot 7 set off (Module Failed SCP dnld) |
| CSCtf71990 | Cisco IOS | Call-home message not sent on reload if source-ip-addr is configured |
| CSCtf76561 | Cisco IOS | c2w2c: VSS MEC caching can fail /w vlan change on VS Act, if stdby down |
| CSCtf78122 | Cisco IOS | EAPOL "seen" flag is not set when MAB is pre-empted by 802.1x |
| CSCtf80540 | Cisco IOS | VSS: Memory Leaks with EAP Framework with CTS dot1x/manual links. |
| CSCtf83906 | Cisco IOS | W2.Clix: after apply/remove/re-apply v6 ACL's, TCAM full |
| CSCtf88089 | Cisco IOS | VSS: TB's seen with SSO |
| CSCtf91665 | Cisco IOS | CSCtf56694 creates auth fail retry anomaly |
| CSCtf93027 | Cisco IOS | sup 720 crashes while executing show file desc continously |
| CSCtf93876 | Cisco IOS | "sh plat hardware capacity multicast" does not work after switchover |
| CSCtf98621 | Cisco IOS | Recreating a deleted vlan comes up with "act/lshut" state |
| CSCtg06121 | Cisco IOS | W2.Clix:Active sup crashes on doing ICA reset of the standby vss switch |
| CSCtg08019 | Cisco IOS | Several Malabar-RL under test being reset while perform Sup switch-over |
| CSCtg09360 | Cisco IOS | dot1x security violation with RSPAN configured |
| CSCtg17979 | Cisco IOS | vs_ltl_set_ucast_source_indices slot 19 num_ports 8 fail msgs on bootup |
| CSCtg18269 | Cisco IOS | Event 'soft_reset' is invalid for the current state 'remote_soft_reset': |

| Identifier | Technology | Description |
|---|---|---|
| CSCtg18877 | Cisco IOS | After insert PS2, appear "%C6KENV-SP-4-PSFANFAILED..."messeage. |
| CSCtg20098 | Cisco IOS | SVI needs to be created for EW client to connect to the switch |
| CSCtg26870 | Cisco IOS | Bridge Assurance broken on root port |
| CSCtg29266 | Cisco IOS | Increasing DHCP snooping database size |
| CSCtg30383 | Cisco IOS | vif int address change causing vlan/vpn programming mismatch in sp |
| CSCtg32588 | Cisco IOS | Unknown unicast traffic drop sso with pseudo class config with VPLS TE |
| CSCtg32797 | Cisco IOS | c6k long failover issue with multicast MVPN |
| CSCtg34169 | Cisco IOS | VSS: cannot boot standby after 2nd switchover |
| CSCtg37826 | Cisco IOS | Inter range command doesn't work |
| CSCtg41173 | Cisco IOS | Checkout CSCte68072 (CoPP for VRRP,BFD,GLBP) from w2clix |
| CSCtg41420 | Cisco IOS | PIM/BGP takes 60-70 sec to establish on ip-tunnel on serial interface up |
| CSCtg44661 | Cisco IOS | ASR router crashes when unconfiguring route-map |
| CSCtg45139 | Cisco IOS | 4sup: vs_ha_slc_sync_startup_config:Getting local startup config failed |
| CSCtg47088 | Cisco IOS | Sticky mac-address entry not removed from running-config |
| CSCtg50990 | Cisco IOS | 6500 DHCPv6 relay does not forward on layer 3 vlan interfaces. |
| CSCtg54603 | Cisco IOS | IPC Standby port not transitioning to Active Ports after RP Switchover |
| CSCtg54691 | Cisco IOS | Met2 is not programmed when p2p gre tunnel is IIF for service reflect gr |
| CSCtg57151 | Cisco IOS | Cat6500 running 12.2933)SXH4 modular IOS crashed without RP crashinfo |
| CSCtg58235 | Cisco IOS | Minor Error @ bootup on multiple 8xCHT1/E1 SPA cards. |
| CSCtg60424 | Cisco IOS | Fast-UDLD:Some ports connecting to VSS stby getting err-disalbed on boot |
| CSCtg63240 | Cisco IOS | cat6500/12.2(33)SXH6 - SNMP-WALK: slow memory leak (SNMP SMALL CHU) |
| CSCtg68012 | Cisco IOS | %SCHED-3-THRASHING: Process thrashing on watched mssg event |
| CSCtg73213 | Cisco IOS | c2w2c - Crash seen on Configuring ATMoMoGRE |
| CSCtg73798 | Cisco IOS | BPDU PW goes down on one side when peer LC is reset twice |
| CSCtg78883 | Cisco IOS | Patch triggers EARL Recovery. |
| CSCtg79692 | Cisco IOS | W2C: Multicast traffic duplicated when OIR card comes back up |
| CSCtg82121 | Cisco IOS | CLIX: Z switchover does not work |
| CSCtg85476 | Cisco IOS | CAT6K NTI ERR and stdby hangs with abortversion while stdby reloading |
| CSCtg85484 | Cisco IOS | No RST packets send to client for an idle out connection with VRF LITE |
| CSCtg89262 | Cisco IOS | Switch sends eapol response packet, during bootup with aaa guarantee fir |
| CSCtg92327 | Cisco IOS | MET entries are not deleted properly |
| CSCtg94067 | Cisco IOS | MLS-MSC ASSERTION FAILED with Bidir traffic drop on ISSU RV |
| CSCtg94220 | Cisco IOS | BIT-SP-4-OUTOFRANGE:bit 50463232 is notin d expectd rangeof 1920 t 8191 |
| CSCtg94601 | Cisco IOS | C4HD1: Continuous TBs @ EthChnl assert failure: on VSS |
| CSCtg98525 | Cisco IOS | ISSU MLS MSC Client(6036) incompatible while issu btn SXI2a->SXI4.FC2 |
| CSCth01912 | Cisco IOS | Tbs @VSL manager on SSO |
| CSCth02812 | Cisco IOS | Unicast flood on ingress asymmetric L2 device after TCN event |

| Identifier | Technology | Description |
|---|---|---|
| CSCth04998 | Cisco IOS | [VSS] DFC installs drop index for MAC-address |
| CSCth05276 | Cisco IOS | VSS: WS-X6716-10GE TestLoopback fails occasinally in slot 2 port 1 |
| CSCth07233 | Cisco IOS | SPA Crypto Connect SSO fails with SVI to Physical int |
| CSCth10626 | Cisco IOS | C2W2C: Memory leak due to OIR of WiSM Module |
| CSCth12206 | Cisco IOS | 6500 with 12.2(33)SXI3 May Not Forward Multicast With SLB Configured |
| CSCth13500 | Cisco IOS | SXH: Member entries missing for port-channel in ifStackTable for SUP32 |
| CSCth13572 | Cisco IOS | C2W2C: WS-X6716-10GE Failed TestMacNotification and reset after VSS SSO |
| CSCth15109 | Cisco IOS | Flowmask conflict between "Intf full flow" and "full flow least" |
| CSCth18024 | Cisco IOS | xconnect: not show pseudowire status syslog on remote PE |
| CSCth23534 | Cisco IOS | 2960: Crash when host is in auth fail vlan and ACS not reachable |
| CSCth23794 | Cisco IOS | Heathland & RR interfaces errdisable with "vlan inte all poli des" cfg |
| CSCth26739 | Cisco IOS | UTIL-3-TREE Data structure error--attempt to remove is seen. |
| CSCth26920 | Cisco IOS | TCL: ungraceful exit from tclsh can leave the Tcl Server running |
| CSCth29861 | Cisco IOS | VSS: Crash at validate_memory/checkheaps after ISSU from SXI3 to SXI4 |
| CSCth29986 | Cisco IOS | ip2tag fragmentation not working with TE tunnel |
| CSCth29993 | Cisco IOS | Upgrade Atlas FPGA for javelin SPAs on 6500 platform |
| CSCth33985 | Cisco IOS | LLDP-MED Network Policy TLV DSCP set to 45 |
| CSCth34752 | Cisco IOS | Cat6k crashes at 'show ip mroute vrf' |
| CSCth35011 | Cisco IOS | memory leak in name_svr.proc on devices running modular IOS |
| CSCth36813 | Cisco IOS | VSL PO goes down while changing the  switch fabric mode |
| CSCth37830 | Cisco IOS | 12.2(33)SXI3 - xconnect traffic stops when neighboring xconnect removed |
| CSCth38120 | Cisco IOS | RIP offset 0 command is not synced to the standby PRE |
| CSCth40444 | Cisco IOS | Tracebacks on inserting 6708 in 6500 with SXI3 |
| CSCth41644 | Cisco IOS | 6716 in performance mode has incorrect input/output rate counters |
| CSCth42709 | Cisco IOS | AToM/ATM AC: pvc cell-packing change causes continious flaps if pw redun |
| CSCth43783 | Cisco IOS | No hardware entries for EoMPLS pseudowire |
| CSCth45241 | Cisco IOS | CE1-CE2 ping is not wroking with GRE tunnel |
| CSCth48435 | Cisco IOS | Tracebacks seen on reduncdancy force with BFD |
| CSCth48803 | Cisco IOS | VS2 - Heathland fast-hello link faills after chg port-grp mode |
| CSCth49187 | Cisco IOS | Alloc-Proc *Dead* in VTPMIB EDIT BUFFER using vtpmib_download_config |
| CSCth52866 | Cisco IOS | Cat6k - changing interface value via SNMP with "parser config cache int" |
| CSCth55383 | Cisco IOS | %EARL-DFC2-2-SWITCH_BUS_IDLE message after "show tech" |
| CSCth55689 | Cisco IOS | ssm ids are down on clearing xconnect before Primary VCs are up |
| CSCth60232 | Cisco IOS | SXH: Port-channel interface flap when changing vlan mask |
| CSCth60242 | Cisco IOS | l2tp-class password <TYPE 0> got encrypted to TYPE 7 in sh run |
| CSCth61317 | Cisco IOS | Message Severity for Noc Payload Crc Error should be 3 |
| CSCth61622 | Cisco IOS | Crash seen on carson split Image |

| Identifier | Technology | Description |
|---|---|---|
| CSCth62957 | Cisco IOS | IPv6 link local packet loops endlessly when L2VPN/RP SPAN configured |
| CSCth63715 | Cisco IOS | VSS:VPLS TE traffic not forwarded after twice switchover |
| CSCth66667 | Cisco IOS | S,G expiry timer is updated during about 2min more after stop S,G stream |
| CSCth69504 | Cisco IOS | 7600 - Small buffer leak on SP due to IGMP snooping |
| CSCth70481 | Cisco IOS | LC frame-relay context missing in advipservices SXI4 Image |
| CSCth73181 | Cisco IOS | Connectivity issue on Cat6k due to index2dvlan table misprogrammed |
| CSCth73553 | Cisco IOS | dot1x phone unregistered during SSO switch-over |
| CSCth74953 | Cisco IOS | SPI Value shown incorrectly as zero for ipsec sa with crypto profiles |
| CSCth76204 | Cisco IOS | TestSPRPInbandPing - No swover/crash after failure threshold reached |
| CSCth76325 | Cisco IOS | OSPFv2 not present in SXI4 base image |
| CSCth79661 | Cisco IOS | MPLS packets missing in TE tunnel accounting |
| CSCth83634 | Cisco IOS | RSTP: Shut/No shut on unrelated neighbour causes root flap |
| CSCth84848 | Cisco IOS | IPv6 OID's not getting polled IPServices feature set |
| CSCth87458 | Cisco IOS | SSH: Memory leak in ssh_buffer_get_string |
| CSCth87937 | Cisco IOS | Crash after configuring 'ip multicast boundary' |
| CSCth92639 | Cisco IOS | Extranet MVPN: the triggered pim join functionality is not working |
| CSCth93066 | Cisco IOS | IPV6 mcast traffic is SW forwded over standby uplink with DCEF-only mode |
| CSCti00272 | Cisco IOS | MultiHost: Web Authentication is triggered after 802.1x authentication |
| CSCti00548 | Cisco IOS | Invalid get detected for Object cpwVcCreateTime |
| CSCti01426 | Cisco IOS | Switch crashes after configuring 'auto qos voip trust' |
| CSCti01971 | Cisco IOS | Active router crashes @ bfd_ipv6_get_local for scaled bfd ipv6 configs |
| CSCti02581 | Cisco IOS | MF:State attribute from previous EAP exchange included in Access Request |
| CSCti04670 | Cisco IOS | Crash found @ sw_mgr_show_feature_base |
| CSCti14287 | Cisco IOS | Unable to display Jian-L CCP and GoreTex SPROM data using show idprom |
| CSCti22519 | Cisco IOS | %ILPOWER-7-DETECT doesnt display with 6500Sup720 wid IOS train 12.2SX |
| CSCti23872 | Cisco IOS | traceroute double hop with set vrf due to double ttl decrement |
| CSCti30359 | Cisco IOS | Client in guest-vlan sending EAPOL start cause security violation on int |
| CSCti32358 | Cisco IOS | linkup is detected earlier than that of the connected device |
| CSCti35158 | Cisco IOS | sup720: L2TP forward L2 PDU  received on flexlink backup interface |
| CSCti35668 | Cisco IOS | IoS "show mod" output display wrong |
| CSCti36805 | Cisco IOS | show facility-alarm status shows negative alarm counts |
| CSCti37172 | Cisco IOS | Ingress SPAN on Sup duplicates packets to ACE module |
| CSCti47250 | Cisco IOS | MVPN: S,G entry not created in mroute table for default-MDT group |
| CSCti48407 | Cisco IOS | Incorrect TTL handling in MPLS traceroute if TTL=1 |
| CSCti53769 | Cisco IOS | Standby reloads continuously when DA exclude link is Lo2147483647 |
| CSCti54470 | Cisco IOS | Cat6K Mcast  Packet loss with IGMP snooping and frequent join/leave |
| CSCti55894 | Cisco IOS | Service Policy applied twice on multilink interface when bounced |

| Identifier | Technology | Description |
|---|---|---|
| CSCti57096 | Cisco IOS | 6500 OIR causes crash w/ service policty on Distributed Etherchannel |
| CSCti60740 | Cisco IOS | crash after disconnect command |
| CSCti64429 | Cisco IOS | Bus Error Crash at fm_process_nf_dbase_clr_timer |
| CSCti65529 | Cisco IOS | Gold diag will fail TestTrafficStress with the Wism installed . |
| CSCti67447 | Cisco IOS | C2wa1-NSF/SSO:- Traffic loss for 8-12 sec with LDP GR enabled |
| CSCti68459 | Cisco IOS | ISSU aborts at runversion due to BOOT var using sup-bootflash |
| CSCti71807 | Cisco IOS | cnfTopFlowsOutputIfIndex returns value 0, instead of destIf |
| CSCti72095 | Cisco IOS | c2wa1: Switch crashed after ISSU runversion from latest sierra to SXI2a |
| CSCti72424 | Cisco IOS | Memory leak in dot1x auth process |
| CSCti83055 | Cisco IOS | CLI: Parser ambiguity with "show platform hardware .." options |
| CSCti83486 | Cisco IOS | c2wa1:Crash @pm_is_rspan_vlan with 7600-SSC with spa-ipsec-2g while boot |
| CSCti84025 | Cisco IOS | VRFs hardware re-mapping causing MLS/CEF inconsistencies |
| CSCti84655 | Cisco IOS | Crash when voice and access VLAN are misconfigured as same VLAN id |
| CSCti84718 | Cisco IOS | CPUHOG @ ipnat_ipalias_check_waitlist+E8 after sh/nosh PBR po int |
| CSCti85352 | Cisco IOS | W1.8: Removing vlan-group from fw mod,vlan-gp already assign get removed |
| CSCti89368 | Cisco IOS | polling xbar using bogus index causes VSAPI-SW1-3-VSAPI_ASSERT &TB |
| CSCti89747 | Cisco IOS | VSS: L2 traffic on healthland gets punted to CPU causing high CPU utilz |
| CSCti93310 | Cisco IOS | With static IGMP outgoing port not programmed in hardware after reload |
| CSCti94107 | Cisco IOS | c2wa1:BOOTUP_TEST_FAIL: Switch 2 Module 1: TestQos failed |
| CSCti99869 | Cisco IOS | IOMEM memleak: DHCP snooping in relay agent environments - Middle buffer |
| CSCtj01590 | Cisco IOS | Unexpected Crypto-routes removals and wrong refcount on RRI routes |
| CSCtj04562 | Cisco IOS | PBR with 'set interface null' causes incorrect tcam programming |
| CSCtj05198 | Cisco IOS | With 2 EIGRP AS, PfR fails to control the route |
| CSCtj06411 | Cisco IOS | crash on single bit parity error with ECC memory |
| CSCtj06432 | Cisco IOS | Crash seen @ msc_destroy_met_set during SSO |
| CSCtj07133 | Cisco IOS | Incorrect switchover to SPT with Multipath configured |
| CSCtj11375 | Cisco IOS | Traffic leaks between secondary vlans when promisucous port is converted |
| CSCtj15088 | Cisco IOS | c2w2:MDEBUG tracebacks @ qm process while applying service policy. |
| CSCtj22529 | Cisco IOS | some mcast shortcut are process switched in ISSU RV. |
| CSCtj27523 | Cisco IOS | On Standby Sup SP, Memory leak seen related to MET |
| CSCtj28482 | Cisco IOS | Cat6k QoS: priority-queue cos-map cmd inserts also rcv-queue cos-map cmd |
| CSCtj38057 | Cisco IOS | QOS ACEs with 'eq' for dst ports not programmed when LOUs/label exceeded |
| CSCtj45154 | Cisco IOS | DUT crashes upon removing dot1x global cmd (auth_mgr_context.c:2375) |
| CSCtj52310 | Cisco IOS | C2wa1: VSS coming up in RPR after switchover w/ dual-active fast-hello |
| CSCtj58219 | Cisco IOS | Standby switch crashes when repl mode is changed to egress in ISSU RV |
| CSCtj59721 | Cisco IOS | %PM_SCP-2-LCP_FW_ERR_INFORM: module 8 is experiencing the following err |
| CSCtj60445 | Cisco IOS | clear crypto sa vrf may be removing sa in the wrong vrf. |

| Identifier | Technology | Description |
|---|---|---|
| CSCtj61261 | Cisco IOS | DFC has misprogrammed i2k_slvan for private vlan after reload |
| CSCtj63031 | Cisco IOS | SNMP syslog trap for OER_MC-5-NOTICE msg is not sent |
| CSCtj69212 | Cisco IOS | MAB Framework leaking memory |
| CSCtj72688 | Cisco IOS | SNMP: need to disable snmp flowcontrol setting for VSL interfaces |
| CSCtj84908 | Cisco IOS | Options data following option82 lost with DHCP-Snooping option82 enabled |
| CSCtj90091 | Cisco IOS | PFC3C fragment entry is not created when ICMPv6 ACL is applied |
| CSCtj91384 | Cisco IOS | IPC Crash Seen In SXH |
| CSCtj91928 | Cisco IOS | C6K PBR set ip nexthop verify-availability w/ tracking & nexthop tunnel |
| CSCtj91961 | Cisco IOS | nvlog contents are cryptic. power_oper_type 62 |
| CSCtj95068 | Cisco IOS | SPAN session gets enabled by snmp set operation |
| CSCtj95352 | Cisco IOS | SUP32 resets with System NMI:**** SP System NMI: reason 0x00000009 |
| CSCtj96421 | Cisco IOS | Leak in SP Buffers. Seen when C6KPWR-SW1_SP-4-PSOUTPUTDROP is logged |
| CSCtj96837 | Cisco IOS | Blank occurred on show run when the system switchover. |
| CSCtj97582 | Cisco IOS | Setting AdminSpeed to autoDetect10100 on cat6500 returns WRONG_VALUE_ERR |
| CSCtk00056 | Cisco IOS | Port Flow-Control Deafult changed after CSCsq14259 on Sup WS-SUP720-3B |
| CSCtk02666 | Cisco IOS | Double dip of scalable EoMPLS traffic on HA switchover |
| CSCtk05146 | Cisco IOS | IPv6 Solicit dropped by RAguard |
| CSCtk05747 | Cisco IOS | TCAM remerge seen on interface up/down, causing 100% CPU |
| CSCtk06057 | Cisco IOS | Enable ESM for sup32 image in sierra |
| CSCtk10374 | Cisco IOS | Crash @ cts_dot1x_authc_supp_info. |
| CSCtk10626 | Cisco IOS | Cat6k - CLNS frames cropped by flexwan |
| CSCtk14496 | Cisco IOS | WA1: system crash when issue {red reload peer} on VS setup |
| CSCtk16232 | Cisco IOS | MVPN traffic software switched due to mtu failure |
| CSCtk31747 | Cisco IOS | RRI route deletion is not proper if same peer ip is across differentFVRF |
| CSCtk31870 | Cisco IOS | FPD upgrade hangs with 'Failed to configure the line card' error message |
| CSCtk31978 | Cisco IOS | c2wa1: VSS Act (SW2) reloads after ISSU LV and AV if NAM card is in SW1 |
| CSCtk32622 | Cisco IOS | WS-X6748-GE-TX May Reset If All Ports Are Shutdown With Interface Range |
| CSCtk33826 | Cisco IOS | C2WA1: ISSU cycle from sierra->SXI with 256PO not working |
| CSCtk36622 | Cisco IOS | Ingress PE routers do not join data MDT of other with connected source |
| CSCtk48038 | Cisco IOS | c2wa1:SP:macedon_b2b_is_failover: msg seen when shut/noshut crypto vlan |
| CSCtk53130 | Cisco IOS | Command "pseudowire" rejected at Virtual-PPP interface with ipv6 |
| CSCtk54650 | Cisco IOS | Modifying IPv6 ACL completely change the ACL configuration |
| CSCtk59111 | Cisco IOS | "txDrops" counter in "show fabric channel-counters" has increasing. |
| CSCtk60169 | Cisco IOS | config sync not happening after setting crcSpanDstPermitListEnabled obj |
| CSCtk61460 | Cisco IOS | Set vlanPortVlan on a port to diff access vlan disconnect IP phone |
| CSCtk64490 | Cisco IOS | c2wa1: XDR ISSU is bypassed on WAN cards while not bypassed on SUP side |
| CSCtk66648 | Cisco IOS | Traceback Spurious memory access pm_get_bcast_supp_discard_counters |

| Identifier | Technology | Description |
|---|---|---|
| CSCtk76633 | Cisco IOS | Wrong FPOE programing after replacing the chassis with different type |
| CSCtl00236 | Cisco IOS | Policy-routing looses dhcp next-hop |
| CSCtl03781 | Cisco IOS | ISSU:ONLINE-SW1_SPSTBY-6-INITFAIL: Module 6: Failed to bring up DFC |
| CSCtl05514 | Cisco IOS | IDSM etherchannel fails after SSO |
| CSCtl45122 | Cisco IOS | CSCsv76509 seen again in SXI4 |
| CSCtl50744 | Cisco IOS | crash on 6k when dot1x accounting feature is turned on |
| CSCtl58697 | Cisco IOS | c2wa1: Swapping WiSM with JIAN fails to bundle JIAN port in LAG |
| CSCtl71282 | Cisco IOS | Traffic of Promiscous port is not sent when sec VLAN mode is changed |
| CSCtl76154 | Cisco IOS | c2wa1: WiSM-1 controller 2 status o/p not available in standalone setup |
| CSCtl82493 | Cisco IOS | c2wa1: After stdby switch reset some Jians and WiSM mgmt ip ping fails |
| CSCtl85771 | Cisco IOS | Both ports in DHD goes to P state on doing SSO in Standby POA |
| CSCtl98884 | Cisco IOS | Crashes noticed in AAA create user (kron /console buffer got corrupted) |
| CSCtn12243 | Cisco IOS | T/b @ icc_send_mcast_request upon bootup |
| CSCtn14939 | Cisco IOS | Crash and Mem Leak under L2 PIM Snooping config after ISSU LoadVer |
| CSCtn16303 | Cisco IOS | The notification was generated incorrectly by ME-C6524GT-8S. |
| CSCtn18962 | Cisco IOS | ospf :s72033-lanbase-mz image missing subsystems |
| CSCtn27004 | Cisco IOS | PS AC/DC input sensor is not detected |
| CSCtn27447 | Cisco IOS | Existing option 82 not overwritten but additionally created |
| CSCtn52363 | Cisco IOS | "channel-group" command missing from member link on module reset |
| CSCtn74068 | Cisco IOS | CSCtl71282 Traffic from Promiscous port isn't switched on mode change |
| CSCtn96481 | Cisco IOS | wrr-queue cos-map can't be configured |
| CSCsi25430 | Infrastructure | JQL: VS2: ActiveVS crash@show_one_proc_one_event_list |
| CSCsr18177 | Infrastructure | Traceback after denied "do" command - 12.2SRB |
| CSCsz45087 | Infrastructure | Incorrect Behavior of Ip sla react-config action-type |
| CSCsz56169 | Infrastructure | crash by memory corruption after executing 'show user' |
| CSCta09049 | Infrastructure | memory leak in encrypto proc or Pool Manager |
| CSCta15808 | Infrastructure | Router Crashes on V6 sanity test:tcrashes in trace_caller() |
| CSCta78502 | Infrastructure | Banner: %r raw data support instead of %s output |
| CSCtb81702 | Infrastructure | OS provisioned CPU Hog detection logic used by BFD/UDLD is not optimal |
| CSCtc51539 | Infrastructure | Router restart due to Watch Dog Timeout when configured with BFD |
| CSCtc51940 | Infrastructure | Error message thrown while executing redirect command |
| CSCtf27594 | Infrastructure | ME-C3750 CPU util. spike to 100% related to BFD |
| CSCtf45681 | Infrastructure | %SCHED-3-SEMLOCKED:SNMP ENGINE after warmstart SNMP ENGINE |
| CSCtg06597 | Infrastructure | Memory leak pointing to hc_counter_force_64bit_cntrs |
| CSCtg17902 | Infrastructure | Logger Process spiking the CPU utilization |
| CSCtg19572 | Infrastructure | Memory leak in two dfs processes |
| CSCtg64468 | Infrastructure | indefinit loops in get_bufferpool_info() & get_buffercachepool_info() |

| Identifier | Technology | Description |
|---|---|---|
| CSCth01674 | Infrastructure | *Dead* memory increasing in (coalesced) |
| CSCti01692 | Infrastructure | RP Crash at ifs_buffer_write upon "show run" |
| CSCti02428 | Infrastructure | Configuration mode lock up |
| CSCti10016 | Infrastructure | Huge amount of disk size loss after format |
| CSCti54695 | Infrastructure | cannot remove snmp-server engineID from running-config |
| CSCti60077 | Infrastructure | Memory leak in IP SNMP Process on cat6k |
| CSCtj31116 | Infrastructure | logging discriminator stops severity filtering |
| CSCtj56019 | Infrastructure | WA1: mibwalk dot1dBridge using mst context does not return correct info |
| CSCsa94774 | IPServices | NAT default breaks Traceroute response |
| CSCsv87146 | IPServices | NAT: router crashes at ipnat_addrpool_find |
| CSCsz05783 | IPServices | NAT translation fails with certain ALG traffic |
| CSCtd73578 | IPServices | Multicast fragments dropped with NAT enabled |
| CSCtd80546 | IPServices | HSRP Virtual mac-addr not flushed after VSS active failover |
| CSCtf75053 | IPServices | 10K is corrupting DHCP-NACK while option 54 is missing in DHCP Request |
| CSCtf88851 | IPServices | tcpConnState in a trap has value zero |
| CSCtf92314 | IPServices | Bus error crash at snmpnat_port_avl_compare |
| CSCtg52885 | IPServices | HSRP on subinterfaces stay stuck in INIT after link flap |
| CSCtg71467 | IPServices | Ospfv3 gets deleted after reload or SSO if virtual ipv6 addr on intf |
| CSCti05663 | IPServices | DHCPACK dropped on relay when Ether-Channel active member link shut down |
| CSCti13845 | IPServices | tftp-server will not serve files of same name in different directories |
| CSCti28796 | IPServices | removing group from class-map type multicast-flows does not change igmp |
| CSCti71843 | IPServices | Ping to NAT outside neighboring interface fails |
| CSCtk95464 | IPServices | Static arp removed after HSRP switchover |
| CSCtf69187 | LAN | changes of Vlan on the sever with VTPv3 is not updated on client with v2 |
| CSCtg25721 | LegacyProtocols | DLSw ER crashes in dlsw_get_sb_from_rhandle |
| CSCtj00728 | LegacyProtocols | ASR crash when configuring DECnet |
| CSCtk95992 | LegacyProtocols | DLSw fails to set up circuit using UDP with peer-on-demand |
| CSCte68677 | Management | PC behind C7941G does not get IP address when connected to 6500 switch |
| CSCtf61362 | Management | Connsistent High CPU on cdp2.iosproc with steady traffic running |
| CSCtf03656 | MPLS | Router crashes @ ip_route_delete after deleting vrf from interface. |
| CSCtf90182 | MPLS | Traffic drop of more than 80sec after multiple SSO with 1PW configured |
| CSCti08115 | MPLS | config-sync failure due to deleted idb with mpls ldp advertise-labels |
| CSCti53167 | MPLS | ION: crash in hw_api_vrf_platform_capability from is_pervrfaggr_enabled |
| CSCti54908 | MPLS | TE-LM leaks bandwidth when Resv's bw not same as Path's bw |
| CSCsy00657 | Multicast | Bus error crash after PIM neighbor DR change |
| CSCtf74238 | Multicast | crash with ip multicast ip multicast boundary command |
| CSCtg91572 | Multicast | duplicate mcast traffic due to non-DR sending PIM join |

| Identifier | Technology | Description |
|---|---|---|
| CSCth02725 | Multicast | Sending PruneEcho message incorrectly, without changing source IP addr |
| CSCth38699 | Multicast | Auto-RP for multicast triggers RP-Discovery with 0 RPs |
| CSCth36280 | QoS | Drop rate for parent hierarchical shaping policy is incorrect |
| CSCeh32332 | Routing | rip lost interface when transmitted-interface flapping |
| CSCek71050 | Routing | CPU Utilization at 100% in BGP Router process in 12.2(33)SRB1 |
| CSCsg18933 | Routing | ATM DSL: RIP default route in Routing Table eventhough not in database |
| CSCsk56788 | Routing | High CPU Proces='BGP Router',when remote neighbor router bgp not active |
| CSCsu88191 | Routing | Cannot remove static route when a similar one is pointing to an intface |
| CSCsx22124 | Routing | CnH: static ip route does not take effect until reconfigured again |
| CSCta23373 | Routing | Eigrp packet size more than ip mtu of gre tunnel |
| CSCtb98722 | Routing | Memory leak on eigrp_timer_init |
| CSCtc25791 | Routing | EIGRP crash when issuing relevant "show" cmd while removing EIGRP config |
| CSCtd81664 | Routing | Not possible to "set ip next-hop" in vrf with import-map |
| CSCtf25357 | Routing | Increased CPU usage in IP-EIGRP: PDM when reflexive ACL configured |
| CSCtf28793 | Routing | bgp aggregate-address suppress-map does not suppress specific prefixes |
| CSCtf33336 | Routing | Offset-list access-list set to 0 in rip configuration. |
| CSCtf64231 | Routing | Inbound route-map change shouldn't be effective immediately |
| CSCtg01873 | Routing | EIGRP summary inherits manually set AD from more specific summary |
| CSCtg18726 | Routing | Network (type-2) LSA is not generated for new interface. |
| CSCtg27206 | Routing | Static route not redistributed by RIP after link flap |
| CSCtg37404 | Routing | RPPREFIXINCONST error comes up continuously due to checksum error |
| CSCtg54878 | Routing | All static routes are not installed in route table |
| CSCth03694 | Routing | C4HD1: Standby keeps reloading due to ISSU incompatibility after reload |
| CSCth05272 | Routing | ISIS/LB removes one route after TE FRR failover and recovery |
| CSCth09200 | Routing | 4948 crashes with "show bgp all peer-group xyz sum" command |
| CSCth20144 | Routing | clear ip route with a /31 address breaks arp table |
| CSCth46888 | Routing | VRRP master sends ARP request with non local MAC as Source |
| CSCth74576 | Routing | NSF for EIGRP  is not configurable in the IPBASE images for SXI4 |
| CSCth84995 | Routing | Crash at fibidb_subblock_message doing issu runversion |
| CSCth89352 | Routing | redistributed static is deleted from rip db when interface down |
| CSCti10518 | Routing | Potential memory leak in ipigrp2_redist_process |
| CSCti20690 | Routing | Request for show running config without displaying ACL configs |
| CSCti30149 | Routing | soft-reconfig route not removed from RIB |
| CSCti32742 | Routing | DSGS4: Stand-by is reloading continuously with Virtual-TokenRing1 int |
| CSCti61949 | Routing | Chunk corruption with MDT enabled VRF |
| CSCti67102 | Routing | Tunnel disables due to recursive routing; holddown timer expires |
| CSCtj00039 | Routing | EIGRP:some prefixes are not being passed from PE to CE router |

| Identifier | Technology | Description |
|---|---|---|
| CSCtj25775 | Routing | Default route redistribution from bgp to rip with wrong metric |
| CSCtj32574 | Routing | Deleting redistribute command into eigrp doesn't get synced to stdby |
| CSCtj34568 | Routing | crash during vrf unconfig - bgp_vpn_impq_add_vrfs_cfg_changes |
| CSCtj46331 | Routing | SNMP walk of atTable leads to high CPU utilization |
| CSCtj47736 | Routing | C4/Mt. Rose:EIGRP/SAF UUT crash  shut/no shut on nei interface |
| CSCtj82292 | Routing | summary-address AD 255 should supress components not advertise summary |
| CSCtj88224 | Routing | Effect of CSCsu96698's improvement "no bgp aggregate-timer" at SRD4 |
| CSCtj99048 | Routing | NSF: type-5 lsa remains even after type-7 becomes unroutable v3 and v2 |
| CSCtk16643 | Routing | EBGP  EBGP Dynamic neighbor not up in multihop scenarios |
| CSCtk64094 | Routing | when MP-BGP is enabled remote-as  statement put on all peers |
| CSCtl00127 | Routing | 'ip security ignore-cipso' not shown as working in 'show ip interface' |
| CSCed66047 | Security | CRYPTO sems inadequately documented |
| CSCek43562 | Security | Not able to close the SSH connection from third party SSH client package |
| CSCek44782 | Security | Double free within mtree code on malloc failure |
| CSCek57606 | Security | set peer <fqdn> dynamic should not resolve for each ACL entry |
| CSCsa99387 | Security | crypt ca truspoint with two-word name disappears after router reload |
| CSCsb40163 | Security | TCP SYN packet from an async interface may fail encapsulation with CBAC |
| CSCsb85643 | Security | Frgmented IP packets fails  b/w Linux Cisco sw vpnclient and IOS ipsec |
| CSCsc56040 | Security | IPSEC router failed to coalesce pak - With certain crypto ACL's |
| CSCsd64304 | Security | Router crashing while  importing certificate:crypto pki import msca-root |
| CSCse42951 | Security | Spurious memory access detected  during CA enrollment |
| CSCsg92744 | Security | IOS SSH client does not display refuse-message when line busy |
| CSCsi24939 | Security | software forced crash at strncmp after 'crypto ca authenticate' |
| CSCsi67268 | Security | Memory leak in Crypto IKMP process when using certificate authentication |
| CSCsk25491 | Security | Bus error crash at mgd_timer_propagate_dbg_info |
| CSCsm27467 | Security | switch crashes if kron used to copy over config via scp |
| CSCsq47980 | Security | Router Crashes @process_run_degraded_or_crash while testing OCSP |
| CSCsz05583 | Security | crypto pki config nvgened before ip config on which it depends - slow |
| CSCsz97833 | Security | PKI: CRL requests get corrupted |
| CSCtg11808 | Security | VSS: Standby supervisor reloads when crypto pki trustpoint removed |
| CSCtg84011 | Security | mac-address on SVI does not work for EIGRP hello packets |
| CSCth79917 | Security | AAA Banner not displayed for a SSH login session |
| CSCti26768 | Security | Bus error while re-configuring a trustpoint |
| CSCte91471 | WAN | NTP v4 takes several hours to sync when multiple servers are configured |
| CSCtf03928 | WAN | NTP packets received but ignored by the NTP process |
| CSCtf88705 | WAN | NTP sync fail after change of interface ip. |
| CSCth66604 | WAN | Modify Action routines of few cli's for ISSU compatibility |

| Identifier | Technology | Description |
|---|---|---|
| CSCti42915 | WAN | Interoperability test for NTPv4 and NTPv3 using authentication |
| CSCti46834 | WAN | NTP sync problem with satellite link |
| CSCti82141 | WAN | ntp pps-discipline CLI gets removed after reload when inverted included |
| CSCtj69886 | WAN | NTP multicast mode not working over MVPN |
| CSCtk10401 | WAN | Local log archive shows 'ntp authentication-key 1 md5 pwd' in clear text |
| CSCtn07728 | WAN | ntp_ipv6 subsystem missing in SUP720 Lanbase image |

# Caveats in Release 12.2(33)SXI and Rebuilds


- Caveats Open in Release 12.2(33)SXI and Rebuilds, page 251
- Caveats Resolved in Release 12.2(33)SXI12, page 252
- Caveats Resolved in Release 12.2(33)SXI11, page 253
- Caveats Resolved in Release 12.2(33)SXI10, page 254
- Caveats Resolved in Release 12.2(33)SXI9, page 256
- Caveats Resolved in Release 12.2(33)SXI8a, page 258
- Caveats Resolved in Release 12.2(33)SXI8, page 258
- Caveats Resolved in Release 12.2(33)SXI7, page 260
- Caveats Resolved in Release 12.2(33)SXI6, page 264
- Caveats Resolved in Release 12.2(33)SXI5, page 269
- Caveats Resolved in Release 12.2(33)SXI4a, page 273
- Caveats Resolved in Release 12.2(33)SXI4, page 273
- Caveats Resolved in Release 12.2(33)SXI3, page 295
- Caveats Resolved in Release 12.2(33)SXI2a, page 300
- Caveats Resolved in Release 12.2(33)SXI2, page 300
- Caveats Resolved in Release 12.2(33)SXI1, page 313
- Caveats Resolved in Release 12.2(33)SXI, page 327


## Caveats Open in Release 12.2(33)SXI and Rebuilds

| Identifier | Component | Description |
|---|---|---|
| CSCue59987 | cat6000-energywise | Input queue size becomes negative with energywise enabled. |
| CSCsu68054 | cat6000-firmware | Cat6k Platform changes required for BGP 4-bytes AS Numbering |
| CSCsv53086 | cat6000-firmware | ipv6 traffic route-cache switched at ipv6ip tunnel (over mpls)c tail end |
| CSCsw50021 | cat6000-firmware | After SSO, FIBIDBINCONS1: An internal software error occurred |
| CSCsw70162 | cat6000-firmware | C2W21: Span port capture duplicated port-channel packets after SSO |
| CSCsx08647 | cat6000-firmware | Traceback at bitlist_validbit within vs_ltl_mgr_proc |
| CSCsx31739 | cat6000-firmware | Outbound policy changes does not reflect by itself in MTR Code base |
| CSCsx76244 | cat6000-firmware | Sup720-Standby continuously reboots on psec mac-move violation with prot |
| CSCsy24099 | cat6000-firmware | get platform-provided x-matrix table on RP |
| CSCsy27228 | cat6000-firmware | Eagle_cnh: Match statement fail to match prefixes |
| CSCsy47965 | cat6000-firmware | FID:for non existent fid ACL on the switch, authz is success |
| CSCta03464 | cat6000-firmware | VPLS VC hardware entry lost upon reroute and TE FRR tunnel shutdown |
| CSCtb95854 | cat6000-firmware | %IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex, on LV & RV |
| CSCte71854 | cat6000-firmware | ACE 30 and ACE 20 reboots in SSO redundency |
| CSCtj52310 | cat6000-firmware | C2wa1: VSS coming up in RPR after switchover w/ dual-active fast-hello |

| Identifier | Component | Description |
|---|---|---|
| CSCtj66981 | cat6000-firmware | MET2 is not programmed for new SR translation rules added in ISSU RV |
| CSCtn12371 | cat6000-firmware | SPA-IPSEC-2GE: XDR-6-XDRLCDISABLEREQUEST / Traceback |
| CSCtn76064 | cat6000-firmware | ACE 30 and ACE 20 reboots in SSO redundency |
| CSCue53095 | cat6000-firmware | ISSU fails between SXJ & SXI on sup32/s720-10G for certain versions. |

## Caveats Resolved in Release 12.2(33)SXI12

### Resolved gsr-boot Caveats

- CSCsv74508—Resolved in 12.2(33)SXI12

  **Symptom:** If a linecard is reset (either due to an error or a command such as hw-module slot reload) at the precise time an SNMP query is trying to communicate with that linecard, the RP could reset due to a CPU vector 400 error.

  **Conditions:** This symptom occurs when the linecard is reset (either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is received.

  **Workaround:** There is no workaround.

### Resolved ospf Caveats

- CSCug34485—Resolved in 12.2(33)SXI12

  **Summary:** Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

  The attacker could trigger this vulnerability by injecting crafted OSPF packets. Successful exploitation could cause flushing of the routing table on a targeted router, as well as propagation of the crafted OSPF LSA type 1 update throughout the OSPF AS domain.

  To exploit this vulnerability, an attacker must accurately determine certain parameters within the LSA database on the target router. This vulnerability can only be triggered by sending crafted unicast or multicast LSA type 1 packets. No other LSA type packets can trigger this vulnerability.

  OSPFv3 is not affected by this vulnerability. Fabric Shortest Path First (FSPF) protocol is not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability.

  **Workaround**: Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130801-lsaospf.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.8/5.8:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:P/E:H/RL:U/RC:C CVE ID CVE-2013-0149 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

| Identifier | Component | Description |
|---|---|---|
| CSCsw43080 | rsr-bridging | Traceback seen @ data_inconsistency_error_with_original_ra |

## Caveats Resolved in Release 12.2(33)SXI11

### Resolved nat Caveats

- CSCtg47129—Resolved in 12.2(33)SXI11

  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:**

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  **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:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

### Resolved Cisco IOS Caveats

- CSCua63614—Resolved in 12.2(33)SXI11

  **Symptom:** When Energywise is enabled on Cat6500 switch, input queue drops can be seen on the interfaces connected to other Energywise neighbors

  **Conditions:** EnergyWise is enabled on Cat6500 and on connected device

  **Workaround:** None

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.3/2.4: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:P/E:U/RL:OF/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Other Resolved Caveats in Release 12.2(33)SXI11

| Identifier | Technology | Description |
|---|---|---|
| CSCth74527 | — | Cat6K: Timing issue with diagnostics corrupt data-forwarding registers |
| CSCub94186 | — | MPLS TE FRR with auto-bandwidth causes hw adj leak/glean on recalc |
| CSCud08574 | — | Vlan Interface over Serial - IPCP nego and Vlan link-up race condition |
| CSCud95251 | IPServices | static nat with vrf looses vrf name after nat translations expire |

| Identifier | Technology | Description |
|---|---|---|
| CSCue21223 | IPServices | Intermitant HSRP hellos not sent w/ IP NAT redundancy configured on SVI |

## Caveats Resolved in Release 12.2(33)SXI10

- CSCty25257—Resolved in 12.2(33)SXI10

  **Symptom:** Packets sent in clear on encrypted link

  **Condition:** Cisco Software in Cisco VPN Services Port Adaptor for Catalyst 6500 contains a vulnerability that could allow an unauthenticated, remote attacker to gain access to sensitive information on a targeted system.

  The vulnerability resides in the encryption library used by the vulnerable software. This library allows a portion of an encrypted packet to be sent unencrypted in the following packet. The vulnerability is specific only when Internet Protocol Security (IPSec) is used, as in the case with Virtual Private Network (VPN) environments. If an unauthenticated, remote attacker could access an encrypted session, the attacker could obtain unencrypted packets that would contain information. This attacker could possibly benefit from this information and possibly launch further attacks.

  **Workaround:** None.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.3/3.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C

  CVE ID CVE-2011-4667 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Other Resolved Caveats in Release 12.2(33)SXI10

| Identifier | Technology | Description |
|---|---|---|
| CSCsz53034 | — | no ingress flows on tunnel interface if nat done before reaching tunnel |
| CSCtg11421 | — | All egress traffic dropped by SIP-400 + BusConnectivityTest failure |
| CSCtj99724 | — | SXI1: Memory leak in "mls-msc Process" |
| CSCto73878 | — | Intermittent PAT Order-of-Operations problem |
| CSCtq38041 | — | InterAS OptAB ASBR crash upon reloading peer |
| CSCtr67722 | — | SP CPUHOG on VSS setup with span session |
| CSCtr92285 | — | MPLS L2VC down as no SSM ID allocated to VC |
| CSCts27161 | — | VSS:standby reloads due to parser return error command: duplex full |
| CSCts90103 | — | Buffer leak on the RP due to IPC messages resulting in a crash |
| CSCts98176 | — | RRI routes missing while IPsec SA is up |
| CSCtt96152 | — | VSS: corrupted Portchannel: LTL missing VSL-link |
| CSCtu22335 | — | On a 6500 after a sup switchover arp inspection fails to forward arp |
| CSCtw61876 | — | IGMPv3 leave results in MCAST packet loss for other receivers |
| CSCtw89269 | — | Ports in 2X1GE-V2 SPA is not coming UP with configured speed |

| Identifier | Technology | Description |
|---|---|---|
| CSCtx12231 | — | Config Sync: Bulk-sync failure due to PRC mismatch in ACL |
| CSCtx50235 | — | SP and RP mutually resetting each other hides the actual crash reason |
| CSCty00274 | — | TLB exception with WAN cards |
| CSCty07538 | — | Incorrect static NAT translation leads to TCP reset |
| CSCty15494 | — | Memory leak in cfib_fibsb_chunk |
| CSCty20876 | — | Show stack does not show correct Information of Last System Crash - SP |
| CSCty20953 | — | Dot1x Re-AuthZl failure with PC connects to AVAYA IP phone |
| CSCty61152 | — | Back out fix for CSCtt66441 |
| CSCty97492 | — | Not all ARP queries going out when port-channel (DEC) is brought back up |
| CSCtz12050 | — | Not possible to disable hol-blocking for X6148 |
| CSCtz45931 | — | MVPN traffic drops when a Port-Channel member module is OIRed |
| CSCtz72735 | — | Mcast traffic on vrf is dropped on shutting one of the paths to the host |
| CSCtz91260 | — | bootup traceback @ %REGISTRY-SPSTBY-3-STUB_CHK_OVERWRITE: |
| CSCua02641 | — | Multicast traffic has second drop during SSO/NSF |
| CSCua08028 | — | Multicast traffic drops under the VRF with IPv6 Family after MVRF upgrad |
| CSCua31268 | — | VRF-lite : ipv4 multicast traffic loss after "no address-family ipv6" |
| CSCua43298 | — | Port loopback mode may not be cleared in corner case |
| CSCtf84248 | AAA | AAA Failover not happening for a directed request |
| CSCti24577 | Infrastructure | Loading a config with banner command creates config sync issues |
| CSCtk36938 | Infrastructure | %SYS-SP-3-CPUHOG @preemption_forced_suspend |
| CSCty04899 | Infrastructure | 6500 - Smart Call Home ignores custom http port configuration |
| CSCtz74540 | Infrastructure | 2 Sup VSS - Mistral interrupt on SP : old active remains in RP Rommon |
| CSCsx28822 | IPServices | Memory leak in the Redundancy inter-device feature (rf task) |
| CSCtq41121 | IPServices | IOS NAT: unable to reconfigure static nat ports after removal |
| CSCtz85702 | IPServices | NAT TCP pptp-control timing-out use_count 1 - entry not removed |
| CSCua43193 | IPServices | Dynamic NAT'g of TCP traffic fails when redudancy VIP is used for NAT |
| CSCua70136 | IPServices | NAT VRF with PAT - PPTP translation failure with dynamic pool |
| CSCub18395 | IPServices | PAT not working when shut/no shut nat+hrsp config interface |
| CSCtc42278 | ISDN | %DATACORRUPTION-1-DATAINCONSISTENCY - ISDN incoming call |
| CSCtd54694 | Management | Switch crashes on Show cdp neighbor detail in some conditions |
| CSCsq83006 | Routing | Port-channel down makes EIGRP SIA |
| CSCtf54561 | Routing | Crash in 'show ip cef vrf' with large number of entries |
| CSCtn02656 | Routing | BGP filtering is incomplete after prefix-list reconfiguration |
| CSCto02448 | Routing | Lost of BGP as-path when clearing BGP soft- all become Local routes |
| CSCtx01476 | Routing | Config Sync: Bulk-sync failure due to PRC mismatch in ACL |
| CSCtz84714 | Routing | IPv6 : snmpwalk on cIpAddressPfxOrigin does not return /64 subnets |
| CSCty26147 | Security | CIPSO pkt. not getting ignored on tunnel interface running 12.2(33)SXI6 |

## Caveats Resolved in Release 12.2(33)SXI9

### Resolved Infrastructure Caveats

- CSCtr91106—Resolved in 12.2(33)SXI9

  **Summary:** A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

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

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 8.5/7:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0384 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Resolved IPServices Caveats

- CSCtr28857—Resolved in 12.2(33)SXI9

  **Summary:** A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  **Note:** The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0382 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCts12366—Resolved in 12.2(33)SXI9

  **Symptoms:** Memory may not properly be freed when malformed SIP packets are received on the NAT interface.

  **Conditions:** None

  **Workaround:** None

  **Further Problem Description:** None.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-2578 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

#### Resolved Cisco IOS Caveats

- CSCts38429—Resolved in 12.2(33)SXI9

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

  **Note:** The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each 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 vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

#### Other Resolved Caveats in Release 12.2(33)SXI9

| Identifier | Technology | Description |
|---|---|---|
| CSCsb02158 | — | RSA-SIG without CA not working with usage-keys on 2811 |
| CSCte44826 | — | memory leak in cfib_alloc_sb running SXH3a |
| CSCth01912 | — | Tbs @VSL manager on SSO |
| CSCtj46927 | — | MF:Access Vlan is removed when 802.1x is enabled on port |
| CSCtq35225 | — | Any new SVIs -> NOT coming up due to RP process SW VLAN RP getting stuck |
| CSCtr73095 | — | LAG data-ports going into Suspended with extend Vlan |
| CSCts26267 | — | Standby VSS switch reloads due to parser return error |
| CSCtt00490 | — | snmpwalk for a N/A DOM-value is returning a bogus value |
| CSCtt17210 | — | On setting crcSrcERSpanLoVlanMask to zero, device goes for a reset. |
| CSCtt18651 | — | cat6000-qos and Traceback after a no shut of a port  system crash |
| CSCtt23872 | — | QoS queueing commands are rejected after manual OIR of module |

| Identifier | Technology | Description |
|---|---|---|
| CSCtt26784 | — | SUP32 crashes on power cycle "registration timer event"at 12.2(33)SXI6 |
| CSCtu38265 | — | MA2 : Crash seen with http auth-proxy |
| CSCtu75030 | — | FTP of exception core dump after crash times out |
| CSCtw44733 | — | command "default interface" break the cos map on other interfaces |
| CSCtw85000 | — | On 7600, 'snmp trap link-status' out of sync on WAN GiGE interface. |
| CSCtx15569 | — | SPA-IPSEC-2G crash packet size above 1800 |
| CSCtx99818 | — | ISSU from SXI6 to SXI9  failed |
| CSCth64138 | AAA | CPU high@'AAA ACCT Proc' session remains after user disconnects |
| CSCts80209 | AAA | Cat6k switch crash on "no login block-for" with login quiet-mode |
| CSCto06915 | Infrastructure | Sup720 remains in ROMMON after SP crash |
| CSCto70125 | Infrastructure | High CPU due to IPSLA tcpConnect probess due to multiple start attempts |
| CSCts71958 | Infrastructure | Last Reload reason in the show version scenario |
| CSCtx68100 | Infrastructure | Reload reason not displayed correctly on some platforms |
| CSCtt70568 | IPServices | PPTP timeout entries are never removed from NAT table. |
| CSCtq73473 | Management | MF: Crash when entering the 'show cdp interface' command |
| CSCtv97307 | MPLS | MLPS LDP flaps with high Tag Control and IPRM CPU utilization |
| CSCtf21128 | Multicast | (S, G) fwd int is NULL while (*, G) is correct |
| CSCtr22007 | QoS | Bus Error crash in MPLS TE LM Process on 7600 |
| CSCtw48209 | QoS | RSVP trap sent when MPLS-TE RSVP session state change may cause crash |
| CSCtf27303 | Routing | 6PE interop: Cisco router sends MP_UNREACH_NLRI in not negotiated SAFI |
| CSCtg79258 | Routing | 33SB7 PE does not send withdraw to CE for 0/0 |
| CSCtr58203 | Routing | Upgrade from 12.2(33)SXH5 to 12.2(33)SXI6 ip local policy w/ VRF |
| CSCto60047 | Security | Chunk corruption crash on trying to abort "show tech" over SSH |

## Caveats Resolved in Release 12.2(33)SXI8a

| Identifier | Technology | Description |
|---|---|---|
| CSCtt26784 | — | SUP32 crashes on power cycle "registration timer event"at 12.2(33)SXI6 |

## Caveats Resolved in Release 12.2(33)SXI8

### Resolved Cisco IOS Caveats

- CSCto72927—Resolved in 12.2(33)SXI8

  **Symptoms:** Configuring an event manager policy may cause a cat4k to hang.

  **Conditions:** Configuring a TCL policy and copying that policy to the device.

  **Workaround:** None.

**PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.7/3.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:H/Au:M/C:N/I:N/A:C/E:F/RL:OF/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Other Resolved Caveats in Release 12.2(33)SXI8

| Identifier | Technology | Description |
|---|---|---|
| CSCsm43012 | — | Speed value changed during the upgrade automatically from 10M to 100M |
| CSCtg96982 | — | Memleak @ bitlist_chunk_alloc on VSS on standby switch |
| CSCth22344 | — | ACE30 sub-module cefcModuleOperStatus returns missing |
| CSCth48435 | — | Tracebacks seen on reduncdancy force with BFD |
| CSCti01971 | — | Active router crashes @ bfd_ipv6_get_local for scaled bfd ipv6 configs |
| CSCtj44456 | — | CSM redundancy sync via CLI causes Standby SUP crash if ANM used |
| CSCtj84234 | — | Packets drop is there when configuring VRF |
| CSCtl77057 | — | TestErrorCounterMonitor can generate false positive on 67XX cards |
| CSCtn68317 | — | Cat6500/SXI: DHCP snooping removed from vlan on module OIR |
| CSCtn81945 | — | MVPN extranet corrupted linkage |
| CSCto90846 | — | Tunnel I/F and Vlan I/F stucked on output and dropped packets on Cat6k. |
| CSCto99774 | — | Crash in vtp mib |
| CSCtq24526 | — | Memory corruption crash in crypto code |
| CSCtq48027 | — | MVRP: Traffic is NOT flowing in the netwok with MVRP enabled |
| CSCtq54944 | — | Minor Error and port down on Failover from SXH2a to SXJ in RPR mode |
| CSCtq61884 | — | DHCP snooping for unicast not working to HSRP DMAC |
| CSCtq80394 | — | mroute entry not create for sparse default-MDT group |
| CSCtq86628 | — | Traceback at SSO SCHED-SW2_SP-7-WATCH uninitialized boolean "rf task" |
| CSCtq94581 | — | voice domain cannot authc when port-security is enabled (MDA mode) |
| CSCtr03012 | — | On SSO, Mcast RPF-MFD fails only with static join @ RPF i/f |
| CSCtr26476 | — | cat6k not always putting the link going to VS sup to FWD via uplinkfast |
| CSCtr46076 | — | crash due to: terminated due to signal SIGBUS, Bus error: MF |
| CSCtr47317 | — | Span replication loop after switchover on Service Module |
| CSCtr50629 | — | Entity Display MIB shows incorrect ACTIVE & POWER MGMT LED status in VSS |
| CSCtr51180 | — | IPSEC-2G in CC on subif reprograms badly icpu vlan map on change |
| CSCtr51517 | — | SSH UNEXPECTED_MSG debugs do not display IP address |
| CSCtr52081 | — | packet storm with external loop on dot1x/mab ports in singlehost mode |
| CSCtr61390 | — | Standby SUP crash @ when its booting with SXI and SXJ image |
| CSCtr67276 | — | PBR within a VRF with object tracking not working on Cat6k |
| CSCtr68112 | — | SW installed NF entry does not get updated when next-hop sends garp |

| Identifier | Technology | Description |
|---|---|---|
| CSCtr84253 | — | cat6k rapidly exhausts system buffers |
| CSCts15934 | — | VSS: MALLOC failure reported by diag_display_fpoe_entries |
| CSCts57516 | — | EzVPN server disconnects all PATed clients |
| CSCts66142 | — | Reconfiguring "mls ip multicast stub" config does not program tcam |
| CSCts91215 | — | after Sup OIR the SPA cards show as online diagnostic state unknown |
| CSCtt21565 | — | QoS: bandwidth remaining percent of non-LLQ policy is not reflected |
| CSCtb89424 | Infrastructure | Crash at saaEventProcessor |
| CSCsb70368 | IPServices | Bus error at ipnat_delete_entry with PPTP-TCP entry deletion |
| CSCtn07696 | IPServices | 6506-E/Sup720 crash related to SYS-3-URLWRITEFAIL: and TCP-2-INVALIDTCB |
| CSCtq14817 | IPServices | Traceback seen @ ipnat_pptp_client_inside |
| CSCtr16396 | IPServices | TAC+ Code Incorrectly Implements timeout for tacacs-server timeout |
| CSCts00341 | IPServices | CLI requiring DNS lookup cannot be configured when in SSO mode |
| CSCtg48785 | LegacyProtocols | sh x25 hunt-group causes %DATACORRUPTION-1-DATAINCONSISTENCY: copy error |
| CSCtr88242 | Multicast | PIM-SM doesn't trigger Join message when RPF is changed |
| CSCsg83966 | Routing | Import MAP:sh ip bgp vpnv4 vrf does not show all entities |
| CSCtn78663 | Routing | Cat6k No ICMP Mask Reply |
| CSCtq62273 | Routing | Configuring IPV6 crashes the router. |
| CSCts16133 | Routing | Sup720 may crash after rebuilding object-group configuration |
| CSCts43881 | Routing | Unexpected RIP route leak/redistribution |
| CSCsr96084 | Security | %SYS-6-STACKLOW: Stack for process NHRP running low, 0/6000 |

## Caveats Resolved in Release 12.2(33)SXI7

### Resolved Cisco IOS Caveats

- CSCtj22354—Resolved in 12.2(33)SXI7

  **Symptom:** System may crash when receiving LLDPDUs.

  **Conditions:** Incoming LLDPDUs with more than 10 LLDP MA(Management Address) TLVs

  **Workaround:** Disable LLDP MA TLV sending on the peers.

  **Further Problem Description:** Currently LLDP supports 10 MA TLVs per LLDP neighbor entry, however, it is not processed properly when more than 10 MA TLVs are received.

- CSCtn76183—Resolved in 12.2(33)SXI7

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

  Cisco has released free software updates that address these vulnerabilities. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

  **Note:** The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes 9 Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. 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 September 2012 bundled publication.

  Individual publication links are in the "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

- CSCtq36327—Resolved in 12.2(33)SXI7

  **Symptom:** A loop between a dot1x enabled port and another a)dot1x enabled port configured with open authentication or b) non-dot1x port, will create a spanning-tree bpdu storm in the network.

  **Workaround:** Avoid creating a loop.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2011-2057 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCtq36336—Resolved in 12.2(33)SXI7

  **Symptom:** An external loop between 2 dot1x enabled ports can cause a storm of unicast EAPoL pdus in the network.

  **Workaround:** Avoid creating a loop.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2011-2058 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

#### Other Resolved Caveats in Release 12.2(33)SXI7

| Identifier | Technology | Description |
|---|---|---|
| CSCsd46369 | AAA | IP source address on packets to TACACS server is wrong |
| CSCsi83685 | AAA | AAA fallback to radius causes GET_PASSWORD debug message |
| CSCsl45701 | AAA | TACACS+ per VRF authen failing: Address already in use |

| Identifier | Technology | Description |
|---|---|---|
| CSCtl54415 | AAA | win11(FIT) - dut crashed after trying to ssh to the dut with no key |
| CSCtl77241 | AAA | MF: webauth login triggers switch crash |
| CSCsk94501 | — | AUTHPROXY: info timestamp array size not the same as max-login-attempts |
| CSCsm36855 | — | %MCT1E1-3-TIMEOUT: TB@ cte1_wait_for_linkrec_ready while unconfig chn gr |
| CSCsr95189 | — | VSS standby switch reset parser error in IDSM config command |
| CSCsu06967 | — | auth-proxy-banner must not be displayed on result page |
| CSCsu65095 | — | switch crash w traceback after applying "eou rev all" |
| CSCtb05389 | — | Alignment errors seen when IKE phase1 failed due to malformed ike packet |
| CSCtc99947 | — | Switch drops DHCP INFORM packets from DHCP client |
| CSCtd58259 | — | sw voice vlan - port removed from STP if snmpset commands are executed |
| CSCtg09619 | — | Web Auth host gets dropped after DHCP renewal with DHCP snooping enabled |
| CSCtg17979 | — | vs_ltl_set_ucast_source_indices slot 19 num_ports 8 fail msgs on bootup |
| CSCtg32797 | — | c6k long failover issue with multicast MVPN |
| CSCtg47088 | — | Sticky mac-address entry not removed from running-config |
| CSCth31231 | — | dACL for MAB still applied for dot1x users |
| CSCti28450 | — | Show auth session port...and oid returns different results |
| CSCti30359 | — | Client in guest-vlan sending EAPOL start cause security violation on int |
| CSCtj84500 | — | Cat6500 - Locked semaphore after config change for CSM WS-X6066-SLB |
| CSCtk63049 | — | Bulk-sync failure due to PRC mismatch due to mls sampling interface |
| CSCtl42871 | — | Show Transceiver Detail Should Show N/A for all fields Instead of 0.00 |
| CSCtl58831 | — | small buffer leak on WS-X6708-10GE |
| CSCtl71282 | — | Traffic of Promiscous port is not sent when sec VLAN mode is changed |
| CSCtl75972 | — | CPUHOG for "Virtual Exec" seen when removing/adding ACL on VSS |
| CSCtl83800 | — | Erspan traffic flows after shut/no shut of src port even if session down |
| CSCtn12198 | — | Watchdog timeout after enabling NetFlow |
| CSCtn15098 | — | MF:IDH:Local session timer does not kick in if AAA timer is disabled. |
| CSCtn27420 | — | MF: device tracking causes duplicate address warning on Windows |
| CSCtn60147 | — | 6500 SXI - L2 traffic is policed when CoPP is enabled |
| CSCtn74068 | — | CSCtl71282 Traffic from Promiscous port isn't switched on mode change |
| CSCto34230 | — | RRI: C6K not remove routes when SAs removed by DPD. |
| CSCto53223 | — | VSPA\>WS-IPSEC-3 : Failure in VRF Mode acting as EzVPN Server |
| CSCto98855 | — | Supervisor crashes in VS mode when VSL LC crashes |
| CSCtq06964 | — | Old Phase ID is used when EzVPN client connect with different ID |
| CSCtq26766 | — | SUP720-3B crash due to large number of IGMP reports received |
| CSCtq26863 | — | Authentication session information sticks when port shut down |
| CSCtq48386 | — | Authfail->Guest, show cmd is incorrect |
| CSCtq64820 | — | 6500 SP crash at cmfi_frr_process_stats_counters |

| Identifier | Technology | Description |
|---|---|---|
| CSCtq65338 | — | CDP Bypass allows cisco ip phone to bypass aaa in all host-modes.MUSTFIX |
| CSCtq72873 | — | MF: Crash @ eap_auth_fail |
| CSCtr10155 | — | Crash following defaulting an interface configuration in a port-channel |
| CSCee38838 | Infrastructure | kadis timer abort reloads router |
| CSCta78502 | Infrastructure | Banner: %r raw data support instead of %s output |
| CSCtn78758 | Infrastructure | Crash on Modular IOS on cat6k |
| CSCtq46758 | Infrastructure | process_reschedule_test should not reschedule with mempool_locks_held |
| CSCtq68778 | Infrastructure | After ISSU complete,  the reload reason line in "sh version" is missing |
| CSCtg16573 | — | "%DOT1X_SWITCH-SPSTBY-5-ERR_VLAN_NOT_FOUND" on defaulting MDA port |
| CSCtl24871 | — | GLBP virtual mac not programmed in tunnel internal vlan |
| CSCtl88070 | — | IPv6 VRF configuration causes software punt for global uRPF |
| CSCtn11825 | — | MVRP error disables L3 interface part of 6148A LC when match registerN/A |
| CSCto56118 | — | ACL: Adding a duplicate ACE via an object-group is not rejected |
| CSCtr13929 | — | Primary member link changing with addition of new member to bundle |
| CSCtk47601 | IPServices | SSO failure for cmd ipv6 dhcp test relay forward add 2147483647 cisco123 |
| CSCtl21288 | IPServices | NAT: "%Port xx is being used by system" even after the CSCtd16493 fix |
| CSCtl74114 | IPServices | NAT: static PAT breaks dynamic PAT if they both use the same IP address |
| CSCtn21561 | IPServices | NAT crash while trying to translate DNS reply from an egress interface |
| CSCtl52345 | LegacyProtocols | C3825 bounces back packets with non-owned MAC strangely |
| CSCto68456 | Management | odr incorrectly installs default route out of an L2 interface. |
| CSCsd39315 | PPP | distributed multilink bundle should never show no frags rcvd |
| CSCsv04412 | PPP | %MCT1E1-3-TIMEOUT while deleting bundle with CHT1E1 SPA |
| CSCej87096 | Routing | Redistribute OSPF command messed up |
| CSCek39299 | Routing | BGP-NSR:stby keep reset after bulk sync for bgp dampening CLI |
| CSCsz56498 | Routing | IPv6 route config is not taken into ipv6 routing table |
| CSCtg74011 | Routing | BGP -IPv6 and IPv4 Capability |
| CSCtj88224 | Routing | Effect of CSCsu96698's improvement "no bgp aggregate-timer" at SRD4 |
| CSCtn96521 | Routing | When the Spoke (dynamic) peer-group is configured before the iBGP (stati |
| CSCto00796 | Routing | BGP stops advertising RT  extended community to peers in a peer-group |
| CSCto31265 | Routing | OSPFv3:ABR does not translate Type7 when primary Type7 is deleted |
| CSCto46716 | Routing | TE tunnel is not added into RIB even its found in forwarding-ad and OSPF |
| CSCtq43285 | Routing | Routing churn BGP-EIGRP in VRF-Lite |
| CSCsi67268 | Security | Memory leak in Crypto IKMP process when using certificate authentication |
| CSCtk10401 | WAN | Local log archive shows 'ntp authentication-key 1 md5 pwd' in clear text |

## Caveats Resolved in Release 12.2(33)SXI6

### Resolved AAA Caveats

- CSCth25634—Resolved in 15.0(1)SY

  **Symptoms:** Password is prompted for twice for authentication.

  **Conditions:** This issue occurs when login authentication has the line password as fallback and RADIUS as primary. For example:

  ```
  aaa authentication login default group radius line
  ```

  **Workaround:** Change the login authentication to fall back to the enable password that is configured on the UUT. For example:

  ```
  enable password <keyword>
  aaa authentication login default group radius enable
  ```

  **Further Information:** The fix for this bug also fixes an unrelated problem that may allow unauthorized users access to EXEC mode if the "line" authentication method is configured with fallback to the "none" authentication method. In other words, if the following is configured:

  ```
  aaa new-model
  aaa authentication login MYMETHOD line none

  line con 0
    login authentication MYMETHOD
    password <some password>
  ```

  then users providing the wrong password at the password prompt will be granted access.

  This issue was originally introduced by Cisco Bug ID CSCee85053, and fixed in some Cisco IOS releases via Cisco Bug IDs CSCsb26389 ("Failover for aaa authentication method LINE is broken") and CSCsv06823 ("Authentication request doesnt failover to any method after enable"). However, the fix for this problem was not integrated into some Cisco IOS releases and this bug (CSCth25634) takes care of that.

  Note that Cisco Bug ID CSCti82605 ("AAA line password failed and access to switch still passed") is a recent bug that was filed once it was determined that the fix for CSCee85053 was still missing from some Cisco IOS releases. CSCti82605 was then made a duplicate of this bug (CSCth25634) since the fix for this bug also fixes CSCti82605.

### Resolved Infrastructure Caveats

- CSCte01606—Resolved in 12.2(33)SXI6

  **Symptoms:** When Bidirectional Forward Detection (BFD) is enabled, issuing certain CLI commands that are not premption safe may cause the device to restart. This condition has been seen when issuing commands such as "show mem" or"show mem frag detail".

  **Conditions:** The issue may occur if BFD is enabled on a device that utilizes Pseudo Preemption to implement this feature. The device must be running an affected software build.

  **Workaround:** Disable BFD

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.4/3.8:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:S/C:N/I:N/A:C/E:H/RL:OF/RC:C

  CVE ID CVE-2010-3049 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCti25339—Resolved in 12.2(33)SXI6

  **Symptoms:** Cisco IOS device may experience a device reload.

  **Conditions:** This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  **Workaround:** There is no workaround.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2010-3050 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

#### Resolved LegacyProtocols Caveats

- CSCth69364—Resolved in 12.2(33)SXI6

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw.

#### Other Resolved Caveats in Release 12.2(33)SXI6

| Identifier | Technology | Description |
|---|---|---|
| CSCsb46724 | AAA | AAA server group doesnt failover with mismatched keys for login |
| CSCsc49958 | AAA | aaa authentication fallback to enable caches previously typed password |
| CSCti00011 | AAA | MF: NAD sending previous state attribute in EAP Identity request |
| CSCsw52498 | — | Extended unsuccessfull dot1x authentication causes red Sup5 to core dump |
| CSCsz72735 | — | VSS STP state change over port channel |
| CSCta15276 | — | auth_mgr_get_authotization_feature_name returns incorrect value |
| CSCta86571 | — | c4hd1: BIT-SW2_SP-4-OUTOFRANGE TB seen during SS0 |
| CSCtd70009 | — | IPphone second port notification not clearing session on 2k |
| CSCte01410 | — | lost packests between FWSM and engine when switchover by SSO |
| CSCte75473 | — | SPA-IPSEC-2G is dropping ISIS L2 packets |
| CSCtf25141 | — | Mem leak seen msc_create_met_set, msc_update_met_set & hal_send_met_job |
| CSCtf78122 | — | EAPOL "seen" flag is not set when MAB is pre-empted by 802.1x |
| CSCtf80540 | — | VSS: Memory Leaks with EAP Framework with CTS dot1x/manual links. |
| CSCtf91665 | — | CSCtf56694 creates auth fail retry anomaly |
| CSCtg09360 | — | dot1x security violation with RSPAN configured |

| Identifier | Technology | Description |
|---|---|---|
| CSCtg45139 | — | 4sup: vs_ha_slc_sync_startup_config:Getting local startup config failed |
| CSCtg54691 | — | Met2 is not programmed when p2p gre tunnel is IIF for service reflect gr |
| CSCtg94601 | — | C4HD1: Continuous TBs @ EthChnl assert failure: on VSS |
| CSCth23534 | — | 2960: Crash when host is in auth fail vlan and ACS not reachable |
| CSCth29986 | — | ip2tag fragmentation not working with TE tunnel |
| CSCth35011 | — | memory leak in name_svr.proc on devices running modular IOS |
| CSCth41644 | — | 6716 in performance mode has incorrect input/output rate counters |
| CSCth45241 | — | CE1-CE2 ping is not wroking with GRE tunnel |
| CSCth49187 | — | Alloc-Proc *Dead* in VTPMIB EDIT BUFFER using vtpmib_download_config |
| CSCth61317 | — | Message Severity for Noc Payload Crc Error should be 3 |
| CSCth69504 | — | 7600 - Small buffer leak on SP due to IGMP snooping |
| CSCth74953 | — | SPI Value shown incorrectly as zero for ipsec sa with crypto profiles |
| CSCth79661 | — | MPLS packets missing in TE tunnel accounting |
| CSCth93066 | — | IPV6 mcast traffic is SW forwded over standby uplink with DCEF-only mode |
| CSCti22519 | — | %ILPOWER-7-DETECT doesnt display with 6500Sup720 wid IOS train 12.2SX |
| CSCti32358 | — | linkup is detected earlier than that of the connected device |
| CSCti33299 | — | RP crash due to TLB exception following crypto-map configuration |
| CSCti37172 | — | Ingress SPAN on Sup duplicates packets to ACE module |
| CSCti47250 | — | MVPN: S,G entry not created in mroute table for default-MDT group |
| CSCti48407 | — | Incorrect TTL handling in MPLS traceroute if TTL=1 |
| CSCti54470 | — | Cat6K Mcast  Packet loss with IGMP snooping and frequent join/leave |
| CSCti57096 | — | 6500 OIR causes crash w/ service policty on Distributed Etherchannel |
| CSCti60740 | — | crash after disconnect command |
| CSCti65529 | — | Gold diag  will fail TestTrafficStress  with the Wism installed . |
| CSCti68459 | — | ISSU aborts at runversion due to BOOT var using sup-bootflash |
| CSCti72424 | — | Memory leak in dot1x auth process |
| CSCti89368 | — | polling xbar using bogus index causes VSAPI-SW1-3-VSAPI_ASSERT &TB |
| CSCti93310 | — | With static IGMP outgoing port not programmed in hardware after reload |
| CSCtj01590 | — | Unexpected Crypto-routes removals and wrong refcount on RRI routes |
| CSCtj04562 | — | PBR with 'set interface null' causes incorrect tcam programming |
| CSCtj06411 | — | crash on single bit parity error with ECC memory |
| CSCtj06432 | — | Crash seen @ msc_destroy_met_set during SSO |
| CSCtj07133 | — | Incorrect switchover to SPT with Multipath configured |
| CSCtj27523 | — | On Standby Sup SP, Memory leak seen related to MET |
| CSCtj28482 | — | Cat6k QoS: priority-queue cos-map cmd inserts also rcv-queue cos-map cmd |
| CSCtj38057 | — | QOS ACEs with 'eq' for dst ports not programmed when LOUs/label exceeded |
| CSCtj45154 | — | DUT crashes upon removing dot1x global cmd (auth_mgr_context.c:2375) |

| Identifier | Technology | Description |
|---|---|---|
| CSCtj58219 | — | Standby switch crashes when repl mode is changed to egress in ISSU RV |
| CSCtj59721 | — | %PM_SCP-2-LCP_FW_ERR_INFORM: module 8 is experiencing the following err |
| CSCtj60445 | — | clear crypto sa vrf may be removing sa in the wrong vrf. |
| CSCtj61261 | — | DFC has misprogrammed i2k_slvan for private vlan after reload |
| CSCtj69212 | — | MAB Framework leaking memory |
| CSCtj72688 | — | SNMP: need to disable snmp flowcontrol setting for VSL interfaces |
| CSCtj76591 | — | WS-X6548-GE-TX:Outdiscards is counted on only SPAN dest port |
| CSCtj84789 | — | Additional bridge asic registers need to be removed from TestErrorCounte |
| CSCtj84908 | — | Options data following option82 lost with DHCP-Snooping option82 enabled |
| CSCtj91384 | — | IPC Crash Seen In SXH |
| CSCtj91928 | — | C6K PBR set ip nexthop verify-availability w/ tracking & nexthop tunnel |
| CSCtj91961 | — | nvlog contents are cryptic. power_oper_type 62 |
| CSCtj95068 | — | SPAN session gets enabled by snmp set operation |
| CSCtj96421 | — | Leak in SP Buffers. Seen when C6KPWR-SW1_SP-4-PSOUTPUTDROP is logged |
| CSCtj96837 | — | Blank occurred on show run when the system switchover. |
| CSCtk00723 | — | publish w2clix fw library |
| CSCtk05146 | — | IPv6 Solicit dropped by RAguard |
| CSCtk05747 | — | TCAM remerge seen on interface up/down, causing 100% CPU |
| CSCtk06057 | — | Enable ESM for sup32 image in sierra |
| CSCtk10374 | — | Crash @ cts_dot1x_authc_supp_info. |
| CSCtk10626 | — | Cat6k - CLNS frames cropped by flexwan |
| CSCtk14496 | — | WA1: system crash when issue {red reload peer} on VS setup |
| CSCtk16232 | — | MVPN traffic software switched due to mtu failure |
| CSCtk18890 | — | Protected tunnel went down after FRR kicked in |
| CSCtk31747 | — | RRI route deletion is not proper if same peer ip is across differentFVRF |
| CSCtk31870 | — | FPD upgrade hangs with 'Failed to configure the line card' error message |
| CSCtk31978 | — | c2wa1: VSS Act (SW2) reloads after ISSU LV and AV if NAM card is in SW1 |
| CSCtk32622 | — | WS-X6748-GE-TX May Reset If All Ports Are Shutdown With Interface Range |
| CSCtk33826 | — | C2WA1: ISSU cycle from sierra->SXI with 256PO not working |
| CSCtk36622 | — | Ingress PE routers do not join data MDT of other with connected source |
| CSCtk48038 | — | c2wa1:SP:macedon_b2b_is_failover: msg seen when shut/noshut crypto vlan |
| CSCtk54650 | — | Modifying IPv6 ACL completely change the ACL configuration |
| CSCtk60169 | — | config sync not happening after setting crcSpanDstPermitListEnabled obj |
| CSCtk64490 | — | c2wa1: XDR ISSU is bypassed on WAN cards while not bypassed on SUP side |
| CSCtk76633 | — | Wrong FPOE programing after replacing the chassis with different type |
| CSCtl03781 | — | ISSU:ONLINE-SW1_SPSTBY-6-INITFAIL: Module 6: Failed to bring up DFC |
| CSCtl23494 | — | Dot1x not functioning properly with 3rd party ip-phones |

| Identifier | Technology | Description |
|---|---|---|
| CSCtl45122 | — | CSCsv76509 seen again in SXI4 |
| CSCtl47635 | — | KB lifetime incorrect in "show crypto session detail" |
| CSCtl50744 | — | crash on 6k when dot1x accounting feature is turned on |
| CSCtl54046 | — | Standby Sup crashes@dot1x_get_supp_sb with cts dot1x/manual |
| CSCtl56002 | — | Traceback seen @ "SCP Write Process" |
| CSCtl70909 | — | c2wa1: Type6 password encryption is not wrking in Aggressive Mode |
| CSCtl83517 | — | C2WA1: ISSU cycle from sierra->SXI with 256PO not working - red_mode |
| CSCtl87979 | — | Flexwan card crashes on single bit parity error |
| CSCtn00835 | — | Traceroute via mpls cloud does not show egress PE in 3C mode |
| CSCtn03582 | — | TTL Failure rate-limiter not working |
| CSCtn12243 | — | T/b @ icc_send_mcast_request upon bootup |
| CSCtn14939 | — | Crash and Mem Leak under L2 PIM Snooping config after ISSU LoadVer |
| CSCtn16303 | — | The notification was generated incorrectly by ME-C6524GT-8S. |
| CSCtn27004 | — | PS AC/DC input sensor is not detected |
| CSCtn27447 | — | Existing option 82 not overwritten but additionally created |
| CSCtn43662 | — | Slow memory leak at watcher_create_common (TCP, telnet, watched boolean) |
| CSCtn57039 | — | Memory leak in RADIUS and EAP Framework processes with dot1x configs |
| CSCtn60798 | — | SXI6: System Reload on SSO in met_ha_destroy_tmp_set |
| CSCtn96481 | — | wrr-queue cos-map can't be configured |
| CSCta09049 | Infrastructure | memory leak in encrypto proc or Pool Manager |
| CSCta15808 | Infrastructure | Router Crashes on V6 sanity test:tcrashes in trace_caller() |
| CSCtb81702 | Infrastructure | OS provisioned CPU Hog detection logic used by BFD/UDLD is not optimal |
| CSCtc51539 | Infrastructure | Router restart due to Watch Dog Timeout when configured with BFD |
| CSCtf27594 | Infrastructure | ME-C3750 CPU util. spike to 100% related to BFD |
| CSCtf96250 | Infrastructure | IDBMAN-4-CONFIG_WRITE_FAIL and standby sup crash |
| CSCti60077 | Infrastructure | Memory leak in IP SNMP Process on cat6k |
| CSCtn50281 | Infrastructure | SNMPv3 uses wrong mac for snmp engine ID |
| CSCsv02395 | IPServices | Telnet hostname /vrf <name> does not work |
| CSCtg52885 | IPServices | HSRP on subinterfaces stay stuck in INIT after link flap |
| CSCti05663 | IPServices | DHCPACK dropped on relay when Ether-Channel active member link shut down |
| CSCti28796 | IPServices | removing group from class-map type multicast-flows does not change igmp |
| CSCti71843 | IPServices | Ping to NAT outside neighboring interface fails |
| CSCtl21294 | IPServices | NAT: Port numbers are lost from running cfg if route-map option is used |
| CSCtn27504 | IPServices | track CLI removed after the reload |
| CSCtk95992 | LegacyProtocols | DLSw fails to set up circuit using UDP with peer-on-demand |
| CSCtn12726 | Management | 'show cdp neighbor detail' causes phone outage in dot1x environment. |
| CSCtf90182 | MPLS | Traffic drop of more than 80sec after multiple SSO with 1PW configured |

| Identifier | Technology | Description |
|---|---|---|
| CSCti53167 | MPLS | ION: crash in hw_api_vrf_platform_capability from is_pervrfaggr_enabled |
| CSCsz82587 | QoS | Active crashed on module reset[ES20] with LSM configs |
| CSCsk56788 | Routing | High CPU Proces='BGP Router',when remote neighbor router bgp not active |
| CSCsw63003 | Routing | Continous BGP activity may result in increasing amounts of memory held |
| CSCsx27496 | Routing | Rtr Crash when imported path is selected as mpath & src route del in RIB |
| CSCta23373 | Routing | Eigrp packet size more than ip mtu of gre tunnel |
| CSCtc25791 | Routing | EIGRP crash when issuing relevant "show" cmd while removing EIGRP config |
| CSCtf33336 | Routing | Offset-list access-list set to 0 in rip configuration. |
| CSCtf51640 | Routing | corrupt debug ip packet detail # output |
| CSCth46888 | Routing | VRRP master sends ARP request with non local MAC as Source |
| CSCth89352 | Routing | redistributed static is deleted from rip db when interface down |
| CSCti30149 | Routing | soft-reconfig route not removed from RIB |
| CSCti32742 | Routing | DSGS4: Stand-by is reloading continuously with Virtual-TokenRing1 int |
| CSCti67102 | Routing | Tunnel disables due to recursive routing; holddown timer expires |
| CSCtj34568 | Routing | crash during vrf unconfig - bgp_vpn_impq_add_vrfs_cfg_changes |
| CSCtj46331 | Routing | SNMP walk of atTable leads to high CPU utilization |
| CSCtj47736 | Routing | C4/Mt. Rose:EIGRP/SAF UUT crash  shut/no shut on nei interface |
| CSCtj82292 | Routing | summary-address AD 255 should supress components not advertise summary |
| CSCtj99048 | Routing | NSF: type-5 lsa remains even after type-7 becomes unroutable v3 and v2 |
| CSCtk15123 | Routing | BGP updates not sent out with update group |
| CSCtk64094 | Routing | when MP-BGP is enabled remote-as  statement put on all peers |
| CSCtl00127 | Routing | 'ip security ignore-cipso' not shown as working in 'show ip interface' |
| CSCtl12492 | Routing | Config sync failure after SSO |
| CSCtn78957 | Routing | High CPU seen with large IPv6 neighbor table |

## Caveats Resolved in Release 12.2(33)SXI5

| Identifier | Technology | Description |
|---|---|---|
| CSCtg58029 | AAA | MF:%UTIL-STBY-3-TREE: Data structure error--attempt to remove an unthr |
| CSCth09686 | AAA | "radius-server retry method reorder" removes the server IP upon failover |
| CSCth52843 | AAA | SSO takes 20 to 40 minutes with aaa system accounting |
| CSCti10891 | ATM | 6500 crash due to ATM following upgrade to SXI4 |
| CSCek52883 | — | without IC new peers are added to dyn map instance |
| CSCse29460 | — | distribute-list route-map match source-protocol not working for ospf |
| CSCsg49757 | — | Combining Gig-Sub-intf & crypto connect & vlan with crypto engine |
| CSCsg78501 | — | IKE should not delete established tunnel upon RSA key regeneration |
| CSCsj19194 | — | SP crashes after %PM-3-INTERNALERROR due to switchport flapping |

| Identifier | Technology | Description |
|---|---|---|
| CSCsq45161 | — | High CPU usage on Virtual-Exec due to renewal of DHCP Snooping database |
| CSCsr39340 | — | MPLS packets are not sent across tunnel |
| CSCsr62489 | — | No mask on LC/SP for directly connected prefixes |
| CSCsu67919 | — | SIP crashes - hqf_cwpa_pak_enqueue_local |
| CSCsw36363 | — | SUP32 temperature sensor AUX-1 temperature: N/O |
| CSCsx96689 | — | Bulk sync failed for stp with 802.1x/MDA |
| CSCsz96236 | — | tcp.proc/udp.proc crash at dispatch_manager_pool_context_free |
| CSCta24271 | — | 6500 removes switchport access vlan after a dot1x authentication |
| CSCtc32207 | — | Need better accuracy in RP crash reporting |
| CSCtc69463 | — | Interface input rate is doubled the output when BFD is configured |
| CSCtd84111 | — | IOS SLB doesn't add the CASA input features on an interface |
| CSCtd91871 | — | EZVPN - memory leak  after ungraceful disconnect of client behind PATl |
| CSCte64898 | — | Vacl capture won't work in Ringar when on different Metro |
| CSCte99373 | — | extranet: mrib S,G entry never removed after pim disabled on IIF |
| CSCtf21851 | — | BFD session flap after interface get up status |
| CSCtf33948 | — | PC behind phone authenticates twice. |
| CSCtf61757 | — | 4sup: Power to module in slot 7 set off (Module  Failed SCP dnld) |
| CSCtf93876 | — | "sh plat hardware capacity multicast" does not work after switchover |
| CSCtf98621 | — | Recreating a deleted vlan comes up with "act/lshut" state |
| CSCtg08019 | — | Several Malabar-RL under test being reset while perform Sup switch-over |
| CSCtg26870 | — | Bridge Assurance broken on root port |
| CSCtg34169 | — | VSS: cannot boot standby after 2nd switchover |
| CSCtg37826 | — | Inter range command doesn't work |
| CSCtg41420 | — | PIM/BGP takes 60-70 sec to establish on ip-tunnel on serial interface up |
| CSCtg50990 | — | 6500 DHCPv6 relay does not forward on layer 3 vlan interfaces. |
| CSCtg63240 | — | cat6500/12.2(33)SXH6 - SNMP-WALK: slow memory leak (SNMP SMALL CHU) |
| CSCtg68012 | — | %SCHED-3-THRASHING: Process thrashing on watched mssg event |
| CSCtg85476 | — | CAT6K NTI ERR and stdby hangs with abortversion while stdby reloading |
| CSCtg85484 | — | No RST packets send to client for an idle out connection with VRF LITE |
| CSCtg92327 | — | MET entries are not deleted properly |
| CSCtg94220 | — | BIT-SP-4-OUTOFRANGE:bit 50463232 is notin d expectd rangeof 1920 t 8191 |
| CSCtg98525 | — | ISSU MLS MSC Client(6036) incompatible while issu btn SXI2a->SXI4.FC2 |
| CSCth02812 | — | Unicast flood on ingress asymmetric L2 device after TCN event |
| CSCth04998 | — | [VSS] DFC installs drop index for MAC-address |
| CSCth07233 | — | SPA Crypto Connect SSO fails with SVI to Physical int |
| CSCth10626 | — | C2W2C: Memory leak due to OIR of WiSM Module |
| CSCth12206 | — | 6500 with 12.2(33)SXI3 May Not Forward Multicast With SLB Configured |

| Identifier | Technology | Description |
|---|---|---|
| CSCth13500 | — | SXH: Member entries missing for port-channel in ifStackTable for SUP32 |
| CSCth13572 | — | C2W2C: WS-X6716-10GE Failed TestMacNotification and reset after VSS SSO |
| CSCth15109 | — | Flowmask conflict between "Intf full flow" and "full flow least" |
| CSCth18024 | — | xconnect: not show pseudowire status syslog on remote PE |
| CSCth23794 | — | Heathland & RR interfaces errdisable with "vlan inte all poli des" cfg |
| CSCth26739 | — | Data structure traceback and IDC ERRORS seen in Carson IOS |
| CSCth26806 | — | %EC-SP-5-CANNOT_BUNDLE2 is logged against the auto-gen EC for WiSM |
| CSCth29861 | — | VSS: Crash at validate_memory/checkheaps after ISSU from SXI3 to SXI4 |
| CSCth33985 | — | LLDP-MED Network Policy TLV DSCP set to 45 |
| CSCth37830 | — | 12.2(33)SXI3 - xconnect traffic stops when neighboring xconnect removed |
| CSCth40444 | — | Tracebacks on inserting 6708 in 6500 with SXI3 |
| CSCth48803 | — | VS2 - Heathland fast-hello link faills after chg port-grp mode |
| CSCth55383 | — | %EARL-DFC2-2-SWITCH_BUS_IDLE message after "show tech" |
| CSCth60232 | — | SXH: Port-channel interface flap when changing vlan mask |
| CSCth61622 | — | Crash seen on carson split Image |
| CSCth62957 | — | IPv6 link local packet loops endlessly when L2VPN/RP SPAN configured |
| CSCth63715 | — | VSS:VPLS TE traffic not forwarded after twice switchover |
| CSCth66667 | — | S,G expiry timer is updated during about 2min more after stop S,G stream |
| CSCth70481 | — | LC frame-relay context missing in advipservices SXI4 Image |
| CSCth73181 | — | Connectivity issue on Cat6k due to index2dvlan table misprogrammed |
| CSCth73553 | — | dot1x phone unregistered during SSO switch-over |
| CSCth76204 | — | TestSPRPInbandPing - No swover/crash after failure threshold reached |
| CSCth76325 | — | OSPFv2 not present in SXI4 base image |
| CSCth83634 | — | RSTP: Shut/No shut on unrelated neighbour causes root flap |
| CSCth84848 | — | IPv6 OID's not getting polled IPServices feature set |
| CSCth87458 | — | SSH: Memory leak in ssh_buffer_get_string |
| CSCth87937 | — | Crash after configuring 'ip multicast boundary' |
| CSCth92639 | — | Extranet MVPN: the triggered pim join functionality is not working |
| CSCti01426 | — | Switch crashes after configuring 'auto qos voip trust' |
| CSCti02581 | — | MF:State attribute from previous EAP exchange included in Access Request |
| CSCti15684 | — | PO member and mem count not synched |
| CSCti23872 | — | traceroute double hop with set vrf due to double ttl decrement |
| CSCti36805 | — | show facility-alarm status shows negative alarm counts |
| CSCti53769 | — | Standby reloads continuously when DA exclude link is Lo2147483647 |
| CSCti55894 | — | Service Policy applied twice on multilink interface when bounced |
| CSCti64429 | — | Bus Error Crash at fm_process_nf_dbase_clr_timer |
| CSCti67447 | — | C2wa1-NSF/SSO:- Traffic loss for 8-12 sec with LDP GR enabled |

| Identifier | Technology | Description |
|---|---|---|
| CSCti72095 | — | c2wa1: Switch crashed after ISSU runversion from latest sierra to SXI2a |
| CSCti83486 | — | c2wa1:Crash @pm_is_rspan_vlan with 7600-SSC with spa-ipsec-2g while boot |
| CSCti84025 | — | VRFs hardware re-mapping causing MLS/CEF inconsistencies |
| CSCti84718 | — | CPUHOG @ ipnat_ipalias_check_waitlist+E8 after sh/nosh PBR po int |
| CSCti89747 | — | VSS: L2 traffic on healthland gets punted to CPU causing high CPU utilz |
| CSCti94107 | — | c2wa1:BOOTUP_TEST_FAIL: Switch 2 Module 1: TestQos failed |
| CSCti99869 | — | IOMEM memleak: DHCP snooping in relay agent environments - Middle buffer |
| CSCtj05198 | — | With 2 EIGRP AS, PfR fails to control the route |
| CSCtj15088 | — | c2w2:MDEBUG tracebacks @ qm process while applying service policy. |
| CSCtj22529 | — | some mcast shortcut are process switched in ISSU RV. |
| CSCsi25430 | Infrastructure | JQL: VS2: ActiveVS crash@show_one_proc_one_event_list |
| CSCsr18177 | Infrastructure | Traceback after denied "do" command - 12.2SRB |
| CSCtf45681 | Infrastructure | %SCHED-3-SEMLOCKED:SNMP ENGINE after warmstart SNMP ENGINE |
| CSCtg19572 | Infrastructure | Memory leak in two dfs processes |
| CSCtg64468 | Infrastructure | indefinit loops in get_bufferpool_info() & get_buffercachepool_info() |
| CSCth01674 | Infrastructure | *Dead* memory increasing in (coalesced) |
| CSCti54695 | Infrastructure | cannot remove snmp-server engineID from running-config |
| CSCsa94774 | IPServices | NAT default breaks Traceroute response |
| CSCsv87146 | IPServices | NAT: router crashes at ipnat_addrpool_find |
| CSCsz05783 | IPServices | NAT translation fails with certain ALG traffic |
| CSCtd73578 | IPServices | Multicast fragments dropped with NAT enabled |
| CSCtd80546 | IPServices | HSRP Virtual mac-addr not flushed after VSS active failover |
| CSCte68677 | Management | PC behind C7941G does not get IP address when connected to 6500 switch |
| CSCsy00657 | Multicast | Bus error crash after PIM neighbor DR change |
| CSCtf74238 | Multicast | crash with ip multicast ip multicast boundary command |
| CSCth02725 | Multicast | Sending PruneEcho message incorrectly, without changing source IP addr |
| CSCth38699 | Multicast | Auto-RP for multicast triggers RP-Discovery with 0 RPs |
| CSCsy98768 | PPP | Ping unsuccessful through LAC |
| CSCth36280 | QoS | Drop rate for parent hierarchical shaping policy is incorrect |
| CSCek71050 | Routing | CPU Utilization at 100% in BGP Router process in 12.2(33)SRB1 |
| CSCsg18933 | Routing | ATM DSL: RIP default route in Routing Table eventhough not in database |
| CSCsx22124 | Routing | CnH: static ip route does not take effect until reconfigured again |
| CSCtb98722 | Routing | Memory leak on eigrp_timer_init |
| CSCtd81664 | Routing | Not possible to "set ip next-hop" in vrf with import-map |
| CSCtf25357 | Routing | Increased CPU usage in IP-EIGRP: PDM when reflexive ACL configured |
| CSCtf28793 | Routing | bgp aggregate-address suppress-map does not suppress specific prefixes |
| CSCtf64231 | Routing | Inbound route-map change shouldn't be effective immediately |

| Identifier | Technology | Description |
|---|---|---|
| CSCtg01873 | Routing | EIGRP summary inherits manually set AD from more specific summary |
| CSCtg37404 | Routing | RPPREFIXINCONST error comes up continuously due to checksum error |
| CSCth05272 | Routing | ISIS/LB removes one route after TE FRR failover and recovery |
| CSCth74576 | Routing | NSF for EIGRP  is not configurable in the IPBASE images for SXI4 |
| CSCti10518 | Routing | Potential memory leak in ipigrp2_redist_process |
| CSCti20690 | Routing | Request for show running config without displaying ACL configs |
| CSCtj00039 | Routing | EIGRP:some prefixes are not being passed from PE to CE router |
| CSCtj32574 | Routing | Deleting redistribute command into eigrp doesn't get synced to stdby |
| CSCed66047 | Security | CRYPTO sems inadequately documented |
| CSCsb40163 | Security | TCP SYN packet from an async interface may fail encapsulation with CBAC |
| CSCsz05583 | Security | crypto pki config nvgened before ip config on which it depends - slow |
| CSCtg11808 | Security | VSS: Standby supervisor reloads when crypto pki trustpoint removed |
| CSCtg84011 | Security | mac-address on SVI does not work for EIGRP hello packets |
| CSCti26768 | Security | Bus error while re-configuring a trustpoint |
| CSCtf03928 | WAN | NTP packets received but ignored by the NTP process |

## Caveats Resolved in Release 12.2(33)SXI4a

| Identifier | Technology | Description |
|---|---|---|
| CSCta24271 | — | 6500 removes switchport access vlan after a dot1x authentication |
| CSCth43783 | — | No hardware entries for EoMPLS pseudowire |

## Caveats Resolved in Release 12.2(33)SXI4

### Resolved AAA Caveats

- CSCsg21398—Resolved in 12.2(33)SXI4

  **Symptoms:** The Cisco IOS software image may unexpectedly restart when a crafted "msg-auth-response-get-user" TACACS+ packet is received.

  **Conditions:** This symptom is observed after the Cisco platform had send an initial "recv-auth-start" TACACS+ packet.

  **Workaround:** There is no workaround.

### Resolved Infrastructure Caveats

- CSCtd72456—Resolved in 12.2(33)SXI4

  **Symptoms:** Entering the **show snmp pending** command may cause a Cisco switch to crash.

  **Conditions:** This symptom is observed on a Cisco 3750 switch running Cisco  IOS Release 12.2(50)SE3 configured to send v3 informs, but may affect other platforms.

  **Workaround:** Do not enter the **show snmp pending** command if you have configured informs in the "snmp-server host" statement.

### Resolved Multicast Caveats

- CSCtc68037—Resolved in 12.2(33)SXI4

  **Symptom:** A Cisco IOS device may experience an unexpected reload as a result of mtrace packet processing.

  **Conditions:**

  **Workaround:** None other than avoiding the use of mtrace functionality.

### Resolved Security Caveats

- CSCsg65318—Resolved in 12.2(33)SXI4

  **Symptoms:** Malformed SSH version 2 packets may cause a memory leak.

  **Conditions:** This symptom is observed on a Cisco platform configured for SSH version 2 after it has received malformed SSHv2 packets. The impact of this flaw is that the affected platform may operate in a degraded condition. Under rare circumstances it may reload to recover itself.

  **Workarounds:** Options consist of using SSH version 1 in the interim until the affected platform can be upgraded to a fixed release or permitting only known trusted hosts/networks that can connect to the router by using a VTY access list.

  **Following are examples of the workarounds:**

  Configure SSH version 1

```
Configure SSH version 1
+----------------------
 !-- configure from global config mode
 !
 config t
 !
 ip ssh version 1
 end

VTY access-list
+--------------
 !-- 10.1.1.0/24 is a trusted network that
 !-- is permitted access to the router, all
 !-- other access is denied
 !
 access-list 99 permit 10.1.1.0 0.0.0.255
 access-list 99 deny any
 !
 line vty 0 4
  access-class 99 in
 end
```

  More information about configuring VTY access lists is available in Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T Controlling Access to a Virtual Terminal Line:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/12-4t/sec-cntrl-acc-vtl.html

  More information about SSH on IOS is available in the Configuring Secure Shell on Routers and Switches Running Cisco IOS guide:

  http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

### Resolved Unknown Caveats

- CSCsy16092—Resolved in 12.2(33)SXI4

  **Symptoms:** A router running Cisco IOS or Cisco IOS XE may unexpectedly reload due to watchdog timeout when there is a negotiation problem between crypto peers. The following error will appear repeatedly in the log leading up to the crash:

  .Mar 1 02:59:58.119: ISAKMP: encryption... What? 0?

  **Conditions:** When a malformed payload (Transform payload with vpi length =0) is received and "debug crypto isakmp" is enabled, the error messages are repeatedly seen leading upto the crash.

  **Workaround:** Remove this debug command.

- CSCtc49782—Resolved in 12.2(33)SXI4

  **Symptoms:** Upgrade from 12.2(18)SXF6 to 12.2(33)SXH5 introduced additional vty lines to the running-configuration (vtp line 5 - 15). These new lines do not inherit the security ACL or transports configured by the customer on the old lines (0-4). Switch upgrade caused device to be non-compliant with network security policy defined by customer.

  **Condition:** Software upgrade from 12.2(18)SXF6 to 12.2(33)SXH5.

  **Workaround:** We have to manually configure the ACL for those newly introduced vty lines.

- CSCtc71597—Resolved in 12.2(33)SXI4

  **Symptom:** Currently in EARL7 system, For an IPv6 packet the 96 bytes cover DBUS header (22), Ether header (14), IPv6 harder (40), IPv6 extension headers, and L4 header. That means only 20 bytes (96 - 22 - 14 - 40) are for extension header(s) and L4 header. So even packet with small extension header(s) can use up to 20 bytes that would cause l4_hdr_vld = 0. When that happens, all L4 features cannot be applied and packet would be hardware forwarded based on L3 forwarding result.

  **Conditions:** This issue is present from day one but would cause threat only when ipv6 access-list is configured on any interface and that access-list is containing L4 options.

  **Workaround:** No Workaround

- CSCte83104—Resolved in 12.2(33)SXI4

  **Conditions:** When an ipv6 RACL is confiured on an interface. All packets containing ipv6 optional headers are punted to RP. But if any packets that are sent with no L4 header are also hitting this punt entry present at the top of tcam.

  **Workaround:** No Workaround:

### Resolved WAN Caveats

- CSCtd75033—Resolved in 12.2(33)SXI4

  **Symptom:** Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability. Note: The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section **Further Description** of this release note enclosure.

  **Conditions:** Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

  This is the same as the vulnerability which is described in http://www.kb.cert.org/vuls/id/568372

  Cisco has release a public facing vulnerability alert at the following link:

  http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

The following example identifies a Cisco device that is configured with NTP:

```
router# show running-config | include ntp
ntp peer 192.168.0.12
router#
```

The following example identifies a Cisco device that is not configured with NTP:

```
router# show running-config | include ntp
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

http://www.cisco.com/web/about/security/intelligence/ios-ref.html

**Workaround:** There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

**Note:** NTP peer authentication is not a workaround and is still a vulnerable configuration.

– NTP Access Group

**Warning:** Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access
access-list 1 permit 171.70.173.55
!--- Apply ACE to the NTP configuration
ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

– Infrastructure Access Control Lists

**Warning:** Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well.  The following example covers
!---   an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
```

```
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.

access-list 150 deny udp any
INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example
!--- shown)

interface fastEthernet 2/0
   ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

- Control Plane Policing

  Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

  —Filtering untrusted sources to the device.

  **Warning:** Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

  Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 123

!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 123
```

```
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
   match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
   class drop-udp-class
      drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
   service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

—Rate Limiting the traffic to the device The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

**Warning:** If the rate-limits are exceeded valid NTP traffic may also be dropped.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
   match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates

policy-map rate-udp-traffic
   class rate-udp-class
      police 10000 1500 1500 conform-action transmit
         exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
   service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

**Further Description:** Cisco IOS Software releases that have the fix for this Cisco bug ID, have a behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message: Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command **ntp allow mode private** should be configured. This is disabled by default.

#### Other Resolved Caveats in Release 12.2(33)SXI4

| Identifier | Technology | Description |
|---|---|---|
| CSCin67182 | AAA | Crash in aaa_sg_v2_get_next_server on trying unconfigured radius ser |
| CSCsb17623 | AAA | ALIGN-3-SPURIOUS: Spurious memory access made at error on 3725 (TACACS+) |
| CSCsd82068 | AAA | single-connection to private TACACS+ doesn't recover |
| CSCsf17907 | AAA | LI: not needed attributes in COA are accepted. |
| CSCsi54201 | AAA | IDMGR-3-INVALID_ID error message |
| CSCsq71492 | AAA | IOS device crash or tracebacks at tplus_handle_req_timeout |
| CSCsv13914 | AAA | %ALIGN-3-TRACE: at pppoa_aaa_acct_get_nas_port_details |
| CSCsw79561 | AAA | DROPACCTFAIL: System Accounting fails with tacacs |
| CSCsx07352 | AAA | Console stuck with "authentication failed" on save & reload for sys acco |
| CSCsx15897 | AAA | Cisco 3800 shows symptoms of memory leak in AAA component |
| CSCsx95806 | AAA | Incorrect timeout delay for non-exist radius server |
| CSCsx97093 | AAA | AAA Fails to parse RADIUS callback string ending in = |
| CSCsy20392 | AAA | change default behaviour of accoutning gurantee-first command |
| CSCsy55362 | AAA | Unresponsive Console/VTYs |
| CSCsy61321 | AAA | tac+ acct is not failing over to next server group |
| CSCsz09373 | AAA | POD Reply sent with physical intf ip when req rcvd with loopback intf ip |
| CSCta11120 | AAA | Tacacs single-connect not able to make connection to prev down server |
| CSCta16724 | AAA | IOS release 12.4(24)T breaks partner SCP functionality |
| CSCtb95275 | AAA | Autocommands "access-profile" on vty not executed |
| CSCtc72862 | AAA | C2W2C: Standby router crashes at pagp_switch_mp_create_idb after SSO |
| CSCtc86306 | AAA | Authorization requests not using VRF interface |
| CSCtc94806 | AAA | tacacs-server dns-alias-lookup causes high CPU on TPLUS process |
| CSCtd16343 | AAA | Radius server declared as dead for MAB if server-private in server group |
| CSCte12007 | AAA | System accounting retries are not consistent as expected |
| CSCte69879 | AAA | ip radius source-interface for Acct-on/off not work under aaa group |
| CSCtf23298 | AAA | tacacs-server host " " single-connection causes high CPU utilization |

| Identifier | Technology | Description |
|---|---|---|
| CSCtg40901 | AAA | TACACS single connection crashes @tplus_increase_sock_write_event_count |
| CSCse75697 | ATM | LOKI: ima clock should default to LINE, backout CSCin90422, CSCsb68536 . |
| CSCej00344 | — | Crash when opening new session from router |
| CSCek61184 | — | Memory leak in create_cce_target_class_group |
| CSCsb60761 | — | Spurious memory access with debug crypto ipsec enabled |
| CSCsb95192 | — | RRI with HA doesnt populate the routes correctly - static keyword |
| CSCsd27617 | — | Password encryption aes corruptskeys for  Group names containing _ |
| CSCsg47058 | — | show crypto ipsec client command is not supported |
| CSCsh20336 | — | DMVPN - crypto socket unexpectedly closed for nhrp static entry |
| CSCsj57384 | — | HWIF-QOS-ERR and other types of QoS error messages are seen |
| CSCsk18794 | — | speed and negotiation configuration issue on FE-TX-V2 SPA |
| CSCsk25046 | — | Not all ifIndex'es are in cbQosServicePolicyTable |
| CSCsk49041 | — | crypto_ikmp_utils.c: possible Invalid Pointer Read |
| CSCsk66851 | — | *,G/m entry does not have OIF programmed in HW sometimes |
| CSCsk86410 | — | Abnormal ISAKMP traffic caused an alignment error and traceback. |
| CSCsk88751 | — | Kron CLI Process 'show tech-support password |
| CSCsl94488 | — | Smartports CLI missing in sup32 ipbase image |
| CSCsm63524 | — | SUP32 crashes due to SP hang when it recovers from errdisable |
| CSCsm89642 | — | Bus error crash when executing 'show crypto sessions' |
| CSCso19511 | — | ESM20: No route drops are getting accounted wrongly. |
| CSCso35876 | — | SRB3:New active SP crash at label_entry_get_inlabel |
| CSCso36150 | — | duplicate vlan names causing config-sync failures |
| CSCso79925 | — | EC with enhanced hash method (PFC3C) has no knob to use old method (3B) |
| CSCso99283 | — | Crash with kron configured and show ipc ports |
| CSCsq40205 | — | INTERFACE_API-3-NODESTROYSUBBLOCK:The SWIDB subblock named FM was not re |
| CSCsq63621 | — | SPD classifies OSPF IP Precedence 0 as priority |
| CSCsr13388 | — | To make default debounce timer present at LC to be as configurable |
| CSCsr50134 | — | Router or Linecard may reload at cv6_6pe_frr_stats |
| CSCsr54959 | — | Switch crashes when route-map/policy is unconfigured |
| CSCsr74002 | — | 7600 - VPLS - QinQ- UDLD packet received on qinq flooded to vpls |
| CSCsr99518 | — | Granikos should not init rekey after recieving new outbound SA at QM3 |
| CSCsu31088 | — | Not able to execute any commands under intf after running SPA FPGA bert |
| CSCsu39458 | — | SIP400: LLQ Cndl Policer Always Kicked in for Large Pkts |
| CSCsu51095 | — | OER stop forwarding internet traffic |
| CSCsu81976 | — | IPSEC NAT traversal fails to correctly track SAs |
| CSCsv13243 | — | BFD config causing BGP session to go down |
| CSCsv36976 | — | IKE - Need recovery mechanism when IKE pkts are re-enqueued indefinitely |

| Identifier | Technology | Description |
|---|---|---|
| CSCsv61041 | — | VSS: static mac-address-table entries missing in standby running-config |
| CSCsv82285 | — | Cat6k: UDP port 10000 is opened by default |
| CSCsw28024 | — | Router is getting crashed at crypto_ikmp_cfg_auto_update_parameters |
| CSCsw46893 | — | C2HD1-SI - %CHKPT-4-GET_HUGE_BUF: Client (Event Manager) message seen |
| CSCsx24934 | — | CPU Monitor not heard and ipc TBs on Active VSS switch on issuing Reload |
| CSCsx56011 | — | Switch may crash when issuing "show mac-address-table" |
| CSCsx65088 | — | WiSM on 5.2.157.0 causes %WiSM-5-STATE: Oper-up messages on supervisor |
| CSCsx74064 | — | On modular IOS, SSH on VRF int is allowed irrespective of vrf-also key |
| CSCsx76168 | — | ISSU : hqf ipc Tracebacks on ISSU runversion. |
| CSCsx79111 | — | 7600 MPLS mls cef entry for label imposition has programmed mtu 0 |
| CSCsx81468 | — | CWPA2: Drops CLNS Hello packets |
| CSCsx87562 | — | %SYS-3-TIMERNEG error following configuration change |
| CSCsy04594 | — | Vlan interfaces flap when a root guard port receive superior bpdu |
| CSCsy07709 | — | C2W2: %COMMON_FIB-4-FIBNULLIDB: Missing idb for fibidb Port-channel5A |
| CSCsy27389 | — | EW does not update time accordingly when Daylight Savings time changes |
| CSCsy30937 | — | Modify dual-active fast-hello function for rapid detection and recovery. |
| CSCsy41470 | — | cewEntTable not releasing memory |
| CSCsy49927 | — | IOSd restart seen with RP2@PrepareProcFrameForExecution |
| CSCsy54365 | — | frequent datapath recovery and traffic loss on WS-X6704 with DFC |
| CSCsy58886 | — | NGN:Active crashes when standby booting up on SRC2->SRC3 ISSU |
| CSCsy66678 | — | stp_helper_manipulate_queue: standby SP CPUHOG |
| CSCsy69914 | — | Some lines are omitted when Copy and paste of TCL script in TCL shell |
| CSCsy89677 | — | "% Ambiguous command" returned in the TCLSH for all commands |
| CSCsz01976 | — | Need a cli to dump the rommon environment and unset rommon variable |
| CSCsz04557 | — | When the "set probe frequency" is less than 15 we receive an IP SLA erro |
| CSCsz14273 | — | EEM: CPUHOG and watchdog crash when TCl policy prints large output |
| CSCsz14369 | — | MAB not attempted when RADIUS is available again. |
| CSCsz15989 | — | Event manager applet does not trigger for "clock set" CLI |
| CSCsz23099 | — | Memory leak due to CEF: loadinfos in Collection proc |
| CSCsz23445 | — | %PORT_SECURITY-SP-6-INVALID_SESSION: Invalid Port-Security ISSU Session |
| CSCsz35605 | — | LBL sync failure during removal/addition of cts dot1x from  a trunk port |
| CSCsz42143 | — | WS-X6148A-GE-TX  module fails keepalives when excessive errors on port. |
| CSCsz42241 | — | RRI route deletion broken for non-crypto-map RRI |
| CSCsz47489 | — | Full solution towards the problem faced with service card internal PO as |
| CSCsz52926 | — | Input counters stop after unidirectional receive config change on 6704 |
| CSCsz53124 | — | IPSEC VPN interoperability issue  when IPCOMP compression enabled |
| CSCsz54543 | — | %BFDFSM-3-INVTRANS: seen when bfd is unconfigured |

| Identifier | Technology | Description |
|---|---|---|
| CSCsz74212 | — | incorrenct PS status display after switchover |
| CSCsz76015 | — | C2W2: Need cli to set PF_BIAS to ensure lower slot# Sup boots as active |
| CSCsz90894 | — | Spanning Tree block L2 promiscuous port Leak broadcast traffi |
| CSCta06428 | — | VSS: Active Crash at iccp_test_get_first_mcast_resp_data |
| CSCta06451 | — | PfR:BR Memory leak in export path on 7600 |
| CSCta10075 | — | "clear counters" triggers EEM policy to be run |
| CSCta10402 | — | Tracebacks seen due to BFD PP Process |
| CSCta12382 | — | Udld port config does not sync to standby in rpr-plus mode |
| CSCta13870 | — | Traffic duplicated on Primary and Backup tunnel after FRR |
| CSCta21771 | — | %CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at  0 error on modul |
| CSCta28455 | — | IntMacTx-Err (PI_PN_S_CRC_ERR_CNT) increasing on X6408A-GBIC |
| CSCta29818 | — | Enhanced-Flexwan Module Power Down after Code Upgrade from SXF to SXH |
| CSCta34143 | — | 2nd prefix-list in route-map stanza may not being used |
| CSCta36939 | — | c2w2b:Crash On ISSU Run Version |
| CSCta37465 | — | MAB runs indefinitely, despite received traffic |
| CSCta42669 | — | C2W1: segv exception after portchannel configuration |
| CSCta47293 | — | Enhancement on CDP TLV IP Phone 2nd port status processing |
| CSCta48521 | — | %DATACORRUPTION-1-DATAINCONSISTENCY: copy error |
| CSCta48968 | — | Modular IOS kernel crashinfo has missing information |
| CSCta52689 | — | cat6k crash in RP due to address error with wccp configuration |
| CSCta53157 | — | SPA-4XT3/E3 int in SIP-200 admin-down on standby after fpd upgrade |
| CSCta53466 | — | ISSU on Sup4 causes IPV6 mcast traffic loss to Rcv in Standby uplink |
| CSCta55574 | — | Once in a while catalyst fails to apply to proxyACL with auto mac-check |
| CSCta56305 | — | Detector data port operation status not OK after boot |
| CSCta56890 | — | WiSM LAG and Data Ports flaps on SSO Switchover |
| CSCta57778 | — | auth-mgr/eap::  %IDMGR-3-INVALID_ID: bad id in id_get (bad table id) |
| CSCta61568 | — | Forwarding loop after adding vlan to MST instance |
| CSCta67007 | — | c2hd1:VRF interfaces not shown and not pinging the CE's |
| CSCta68053 | — | time-period does not take effect in configuration archive |
| CSCta71873 | — | Mcast traffic stops flowing across fabric to required fpoes |
| CSCta72199 | — | "aggregate-address advertise-map" not updated dynamically with ION image |
| CSCta74242 | — | VSS: crash due to snmp get after standby chassis reloads |
| CSCta74315 | — | WS-X6324-100FX-MM May Be Inoperable and Have Status "Other" |
| CSCta75226 | — | Mago:ds_isr_cbif ds_num:0 msg on bootup with ip-base image |
| CSCta75882 | — | VSS crashes at platform_reset_by_peer(0x422787e4)+0x6c during sso |
| CSCta76808 | — | add CLI command for medium buffer pool |
| CSCta80024 | — | string repeat crashes router |

| Identifier | Technology | Description |
|---|---|---|
| CSCta83331 | — | APS active and ptrotect circuit show same input counters |
| CSCta84749 | — | Etherchannel should not be allowed if auto qos is enable |
| CSCta94179 | — | Recirculated MPLS packets becasue of egress service policy are dropped |
| CSCta95295 | — | IOMEM depleted when PKI servers unavailable for CRL checking |
| CSCta97265 | — | ip igmp snooping querier is removed from SVI after PC removed. |
| CSCta98108 | — | With NAT, on Netflow database cleanup timer expiry, CPU spikes on 7600 |
| CSCtb03003 | — | MAC table on standby Supervisor not flushed on link change |
| CSCtb04231 | — | Imprecise parity error crash due to mistral timeout |
| CSCtb08846 | — | Address build breakage due to SR commit CSCsz28039 |
| CSCtb09203 | — | active probes partially show up when add new oer-map policy |
| CSCtb15569 | — | VPN-SPA - traffic failed to decrypt due to SecInfo check failure |
| CSCtb16453 | — | ERSPAN /w specific VRF may see traffic routing to default route |
| CSCtb23289 | — | Major temperature alarm has to force system shutdown |
| CSCtb25132 | — | SLB: VSERVER HSRP group name is truncated if any modifcation in VS confi |
| CSCtb27643 | — | cat6000 Medium buffers leak on SP leading to crash |
| CSCtb28032 | — | Changing module corrupts Flex Link |
| CSCtb28712 | — | SPAN Reflector not enabled for WS-SVC-ADM-1-K9 |
| CSCtb31400 | — | BGP sends Route-Refresh request on entering route-map configuration |
| CSCtb34857 | — | crashed seen in xdr_reference |
| CSCtb35917 | — | CSM: HSRP tracking status is not changed from INIT to Standby |
| CSCtb38000 | — | Port error disabled due to ingress pause frames,WS-X6148A-GE-TX |
| CSCtb38547 | — | Incorrect CP0 values and empty kernel variable section in kernel crashin |
| CSCtb41832 | — | C2W23: Port-Channel may not form using LACP across EoMPLS |
| CSCtb44299 | — | Stby RP carsh @ m_requeue |
| CSCtb45475 | — | sh plat hard capacity cpu report system memory usage incorrectly |
| CSCtb47692 | — | VSS: Switch crashed due to EBUS_SEQ_ERROR |
| CSCtb50678 | — | Crash @ registry_add_case with VSS when change from RPR to SSO |
| CSCtb51922 | — | chunk leak fund during " no host-address ip address key-chain CISCO " |
| CSCtb52180 | — | set vrf nvgened while vrf deletion in progress causes standby to reload |
| CSCtb55853 | — | A route-map permits ALL IPv4 routes when "match ipv6" is applied |
| CSCtb55858 | — | No qos rewrite on untrusted port in SXI2 |
| CSCtb55994 | — | EW: Free memory loss when EW is enabled |
| CSCtb58820 | — | RR-B0: Vlan drops observed on Roadrunner at all corners in IOS only |
| CSCtb60330 | — | VTI: Missed DPD ACK on phase 1 expiry causing phase 2 deletion. |
| CSCtb62031 | — | cat6k: High cpu and high inband when reflexive ACL is used with WCCP |
| CSCtb62523 | — | PfR - inside prefixes not learned on cat6k BR |
| CSCtb63352 | — | VSS: With 6KW DC PS, no power to bringup VSL supervisor or linecard |

| Identifier | Technology | Description |
|---|---|---|
| CSCtb65406 | — | QoS ACL May Not Program L4 ports Correctly In TCAM |
| CSCtb66983 | — | Nas-port-type is missing in Access-request |
| CSCtb68478 | — | "Illegal nextSsIndex value" message should be removed |
| CSCtb70344 | — | SH7615 MAC: ucast frames marked as mcast and dropped in offline mode |
| CSCtb70504 | — | Traceback at reg_inv_internal_ha_cs_stdby_out_of_sync |
| CSCtb70578 | — | L2PT incorrectly decapsulates STP PDU for RSPAN causing PVID mismatch |
| CSCtb72638 | — | Ezvpn server not sending split tunneling access-list to client |
| CSCtb78973 | — | PM-SP-3-INTERNALERROR: Port Manager Internal Software Error with dot1x |
| CSCtb83677 | — | Power Deny for pre-standard power on SXI2 or Later |
| CSCtb83776 | — | X6148A-GE-TX-Outdiscard incrementing if queue-limit of priority Q is 0 |
| CSCtb84298 | — | Shadow state of wism PO line protocol down on stdby After OIR of WiSM |
| CSCtb87454 | — | DHCP Rogue Server Detection |
| CSCtb88222 | — | C2W2C: %IDBINDEX_SYNC-4-RESERVE: on LV & RV |
| CSCtb95464 | — | Unable to configure individual interfaces of WiSM on VSS Switch |
| CSCtc01912 | — | EEM: syslog text trigger won't start script if text is in body of debug |
| CSCtc05449 | — | rstp BPDUs are not tunneled over eompls for dfc facing interface |
| CSCtc09913 | — | VTY Process/Telnet connection stuck |
| CSCtc11691 | — | VSS: Switch crashes after loading the sierra 090920 image |
| CSCtc11754 | — | Diags: TestNetflowTCAM intrusive diags test fails with specific configs |
| CSCtc11809 | — | FWSM internal port-channel goes down after SSO forced switchover |
| CSCtc15386 | — | IOS tags VLAN name configuration command as level 1 |
| CSCtc16740 | — | Global BPDUGuard does not work on MVAP ports |
| CSCtc17058 | — | VC stops sending traffic due to duplicate vpn id in port based EoMPLS |
| CSCtc17083 | — | Tunnel decap not programmed, hence traffic RP switched |
| CSCtc19148 | — | CASA: Standby chassis get crashed when Vserver is taken outofservice. |
| CSCtc22217 | — | SPA-8X1FE-TX-V2 negotiation auto and duplex mode issue |
| CSCtc22760 | — | VSS ENH: Immediate reset LC after crash occurrs on stdby chassis LC |
| CSCtc24864 | — | Enable cdp - removed on shut/ no shut dot1q-tunnel interface |
| CSCtc27745 | — | LLDP packets go out tagged if native vlan (not Vlan1) is configured |
| CSCtc28953 | — | Crash on cat6k running MPLS: see resolution note and CSCtc82349 |
| CSCtc30691 | — | Crash/Spurious memory access on privilege ipaddr-object-group/port-objec |
| CSCtc30868 | — | Irregular CPU (peaks) on Cat6500 rtr responder |
| CSCtc30909 | — | TestRwEngineOverSubscription always fails for ACE module |
| CSCtc32375 | — | Crash occurs issuing 'show eigrp service-family external-client |
| CSCtc38716 | — | ME6524 may reset due to single power supply failure |
| CSCtc38771 | — | 12.2SXH: Intermittent BPDU drop over Dot1Q tunnel. |
| CSCtc38905 | — | Disabling IPv6 MLD Snooping breaks IPv4 IGMP and PIM Snooping |

| Identifier | Technology | Description |
|---|---|---|
| CSCtc39052 | — | svclc module command adds firewall module command to configuration |
| CSCtc40420 | — | Basic packet forwarding failed when GRE tunnel is configured |
| CSCtc40724 | — | Multicast packets may get dropped on 6500 when member join mcast group |
| CSCtc49542 | — | VSS: output drops on VS-720 port due to CoS mapping mismatch |
| CSCtc52807 | — | C2HD1-SI: L3 Portchannel's FPOE mask incorrect after SSO |
| CSCtc53375 | — | C2W2B : pagp_switch_sp2mp:idbman_update_mp_delete_agport |
| CSCtc53453 | — | stack members lost energywise config after stack reloading |
| CSCtc53958 | — | "sh run" on Cat6k results in tunnel flapping on non-modular IOS |
| CSCtc54233 | — | Traffic stops between CEs after "clear xconnect all" and SSO in AToM L2L |
| CSCtc54248 | — | CDP neighbors aren't seen on sub-intf when it is disabled on main intf |
| CSCtc54878 | — | NDE direct export packets are checked by egress ACL |
| CSCtc57356 | — | IOS SLB nat pool uses addresses outside range |
| CSCtc58817 | — | [VSS] Incorrect pMASK fpoe on standby causes traffic black-holed |
| CSCtc61506 | — | VSS:VPLS TE traffic dropped on changing data paths. |
| CSCtc63032 | — | Memory allocation failure on 12.2(33)SXI2a using DIA/DHCP Snooping |
| CSCtc64355 | — | Online removal of standby SUP does not reflect to 'show module' command |
| CSCtc65227 | — | standby keeps on reloading when renaming to a profile name with " |
| CSCtc70462 | — | port-security Line-by-Line sync verifying failure |
| CSCtc71996 | — | SSO : Bulk-sync failure at "ip flow-export source" |
| CSCtc78951 | — | C2W2C: port's not recovering from "s" state with non-default native vlan |
| CSCtc79335 | — | Sup Crash on several locations with IP SEC config |
| CSCtc80800 | — | Config sync failure when call-home profile ends with a empty string. |
| CSCtc81612 | — | VSS: Service Module reload triggers corrupted SP program counter |
| CSCtc81772 | — | High cpu utilization with IPv6 ACL |
| CSCtc90469 | — | Supervisor module crashes just after boot up with ACL Deny Test Failure |
| CSCtc91312 | — | Switches crashed when attempting to power on phones after time change |
| CSCtd00423 | — | Spurious memory/crash at adj_from_oce_base after wccp redirect ACL mod |
| CSCtd01483 | — | With fm platform debug on when private-host is config'd the switch crash |
| CSCtd09117 | — | CSM config sync timing out |
| CSCtd11309 | — | VS2 ENTITY-ALARM traps not sent from slave chassis modules |
| CSCtd13853 | — | Linecard interfaces going into UDLD errdisable state on reload |
| CSCtd13970 | — | 'ip cef accounting per-prefix non-recursive' breaks hw-based PBR |
| CSCtd16863 | — | 6500 PoE issues with 1120 line of APs when using dot1x |
| CSCtd18573 | — | EARL-SPSTBY-2-SWITCH_BUS_IDLE: & PF_ASIC dump with 'clear mls qos' |
| CSCtd18807 | — | "set ip next-hop <>" should lookup next hop in VRF when used on VRF int |
| CSCtd21153 | — | Packets are not netflow switched for wccp-L2-redirect(inbound)with hash |
| CSCtd21951 | — | C2W2B: "parser config cache interface" does't work with PO correctly |

| Identifier | Technology | Description |
|---|---|---|
| CSCtd25133 | — | APS K1K2 Bytes Transmission shows channel mismatch |
| CSCtd26829 | — | VSS: Duplicate packets after VSL link change |
| CSCtd26868 | — | RACL blocks L2 switched traffic when adjacency is recirc2.2 |
| CSCtd27768 | — | CISCO-ENTITY-FRU-CONTROL-MIB reports missing module 12.2.(33)SXI2a |
| CSCtd31143 | — | SPA in CC mode with SSO breaks connectivity when other sup comes online |
| CSCtd33166 | — | router crash @ parse_call_action_func |
| CSCtd35521 | — | MVPN PIM neighborship is not formed within vrfs |
| CSCtd39596 | — | OIR of the LC causes bootup diagnostic to fail on TestL3VlanMet |
| CSCtd43793 | — | Web Authentication is triggered after removing fallback configuration |
| CSCtd45736 | — | EOAM:LB functionality is broken from 11/17 due to CSCtb70578 |
| CSCtd46920 | — | Watchdog timeout crash after CPUHOGs in 'Switch IP Host Track Process' |
| CSCtd49505 | — | VSS gets to be multicast traffic blackhole after DAD or switchover |
| CSCtd58314 | — | memory corruption crash with sh ip arp inspect log |
| CSCtd59664 | — | %ERROR: Standby doesn't support this on configuring speed on SIP-400 int |
| CSCtd60858 | — | Spurious accesses while testing dot1x accounting |
| CSCtd63041 | — | %CONST_DIAG-SP-3-HM_FCI_0_STUCK on Mago |
| CSCtd64261 | — | LBL config sync failure for extended vlan name changes |
| CSCtd66689 | — | sip400/ChOC3: Quick shut/no-shut on controller leaves T1s in down state |
| CSCtd69637 | — | Remote end port stays up/up when local port is down/down |
| CSCtd72243 | — | sh int <port> transceiver incorrectly shows Module x doesn't suppot DOM |
| CSCtd72437 | — | Packets punted to software forwarding when route-map is used for NAT |
| CSCtd76204 | — | FPOE_DB-SP-4-ENTRY_USAGE_FULL messages with large vlan config in SXI3 |
| CSCtd78587 | — | Crash when recovering a port which was err-disabled twice |
| CSCtd82666 | — | [VSS]  Incorrect pMASK fpoe on standby causes traffic black-holed |
| CSCtd92043 | — | Ph2 rekey use wrong proxy-id's on cat6k ezvpn ipsec-spa-2g |
| CSCtd93384 | — | Etherchannel on  switch working but interfaces showing shutdown |
| CSCte00934 | — | SLOTCACHE is not updated with "write mem". |
| CSCte03275 | — | Configuring TE tunnels on a causes chunk corruption on the SP. |
| CSCte04768 | — | TestErrorcounter is not counting interrupt on the WS-X67XX linecard |
| CSCte08785 | — | mac notification change history log not seen for deleted mac entries. |
| CSCte15193 | — | c2w2c:"no spanning-tree vlan 16" command is not removed from standby |
| CSCte17961 | — | Web Authentication is triggered after 802.1x authentication |
| CSCte20914 | — | SPAN Reflector not enabled for WS-SVC-ADM-1-K9 : 2nd Commit |
| CSCte21190 | — | WS-X6148A-GE-TX ports 25-32 stop forwarding traffic |
| CSCte21958 | — | Router crashed at l2tun_app_mgr_process when xconnect is configured |
| CSCte28703 | — | cat6k/VSS: fast-hello packet not send to standby SP CPU |
| CSCte30224 | — | Compiled Tcl script crashes when generating a random number |

| Identifier | Technology | Description |
|---|---|---|
| CSCte35598 | — | Extra vlans get created  from MVRP Packet recieved from 3rd party device |
| CSCte40044 | — | SXI: Medium buffer failure followed by 6k crash |
| CSCte40472 | — | FWSM: Private vlan association not syncing on VSS systems from switch |
| CSCte41199 | — | [VSS] MEC port on standby SW appears "missing port in hw" |
| CSCte43407 | — | No %LINK-3-UPDOWN log for SPAN destination port |
| CSCte48967 | — | VSS : isolated pvlan not associated with VRF on DFCs |
| CSCte50279 | — | Need to allow disabling power to empty slots |
| CSCte56366 | — | DSCP values are not mapped to RX priority queue |
| CSCte56437 | — | TCP connection loss due to NAT incorrect translation on cat6500 |
| CSCte71999 | — | Replace ISSU capability negotiation workaround for 4k |
| CSCte72214 | — | ME6500 - Traffic may be dropped on applying cos-map. |
| CSCte76471 | — | sup32 SP hangs on process watchdog |
| CSCte79217 | — | ICCQ never decreases, flow stats affected, (S,G) expires |
| CSCte81230 | — | IP Source Guard feature goes into an incorrect state |
| CSCte83052 | — | Xauth is getting disabled when putting keyring into isakmp profile12.2 |
| CSCte87347 | — | FPGA upgrade of CHT1E1 to 2.8 is not successful |
| CSCte89428 | — | SNMP tty traps not sent |
| CSCte89787 | — | Segment Switch manager Error followed by crash at 'sw_mgr_sm_cm_send_msg |
| CSCte90108 | — | VS:monitor traffic fabric wrong for sw1-2,mod3/ch1 and mod8/ch0 -> RPR |
| CSCte90261 | — | 6500 PoE issues with 1120 and 1230 line of APs when using dot1x |
| CSCte90801 | — | SCP async queue of LC1/LC2 get closed when fan module removed |
| CSCte96453 | — | Switch intermittently crashes bringing up port with energywise level 10 |
| CSCtf02760 | — | Kernel crash (cache error) without any crashinfo generated |
| CSCtf07907 | — | Crash observed @ atom_mgr_activate_dataplane |
| CSCtf08607 | — | %BIT-SW1_SP-4-OUTOFRANGE: bit 1797 is not in the expected range of 1920 |
| CSCtf09903 | — | line vty 5 15 can't be deleted on sup32 |
| CSCtf12294 | — | Memory leak in ceDiagBootUpFailedNotif trap |
| CSCtf15479 | — | VSS: TestMatchCapture failure causing Sup Minor error after manual failo |
| CSCtf16330 | — | DHCP Rogue Server Detection : Multiple DHCPDISCOVER's issue |
| CSCtf23313 | — | C2W2C: Standby Crashes continuously after ISSU LV |
| CSCtf34183 | — | Client can not register to SAFF after correcting wrong user ID |
| CSCtf36557 | — | Cat6K platform side changes related to CSCsk65812 |
| CSCtf37626 | — | Ospf flaps with oversubscription on enhanced flexwan Multilink T1 |
| CSCtf39183 | — | OBFL Master may not be initialized after IOS upgrade from SXF to SXH |
| CSCtf51278 | — | PIM snooping : Router port missing in multicast mac entry |
| CSCtf51541 | — | Mistral reset due to TM_DATA_PARITY_ERROR error |
| CSCtf52407 | — | Sup720 may reload when passing GRE traffic |

| Identifier | Technology | Description |
|---|---|---|
| CSCtf53433 | — | Knob 'platform ipv6 acl punt extension-header' default should be false |
| CSCtf54617 | — | Supervisor fails to come up due to bad compact flash. |
| CSCtf62507 | — | Netflow s/w switched flow not entried if disable/enable ip flow ingress |
| CSCtf64296 | — | SFP on sup720 port 2 show inventory display garbled characters |
| CSCtf71990 | — | Call-home message not sent on reload if source-ip-addr is configured |
| CSCtf75608 | — | No PIM neighbour on newly created SVI |
| CSCtf77734 | — | wrong message is displayed even though cos-map for all ports are removed |
| CSCtf81843 | — | Enh VSS: Fast-Hello interface Allowed commands |
| CSCtf83737 | — | Standby Supervisor crashes on bootup @ fib_vrf_mgr_lookup_vrf |
| CSCtf83906 | — | W2.Clix: after apply/remove/re-apply v6 ACL's, TCAM full |
| CSCtf83970 | — | IO MALLOCFAIL  SSO mode |
| CSCtf88089 | — | VSS: TB's seen with  SSO |
| CSCtf89494 | — | QoS: bandwidth remaining percent of non-LLQ policy is not reflected |
| CSCtf91692 | — | Insertion of 6708/6716 linecard into the chassis resets another linecard |
| CSCtf94697 | — | failed SCP transfer can crash router |
| CSCtf96643 | — | Supervisor crashing qm corruption (Block overrun) |
| CSCtf97963 | — | VSS DFC card miss MN setting, 4Sup: ICS MN ORPOE error |
| CSCtg06121 | — | W2.Clix:Active sup crashes on doing ICA reset of the standby vss switch |
| CSCtg08523 | — | %CONST_DIAG-SP-3-HM_TEST_FAIL:TestIPSecEncrypDecrypPkt seen randomly |
| CSCtg29266 | — | Increasing DHCP snooping database size |
| CSCtg41173 | — | Checkout CSCte68072 (CoPP for VRRP,BFD,GLBP) from w2clix |
| CSCtg58235 | — | Minor Error @ bootup on multiple 8xCHT1/E1 SPA cards. |
| CSCtg73213 | — | c2w2c - Crash seen on Configuring ATMoMoGRE |
| CSCtg78883 | — | Patch triggers EARL Recovery. |
| CSCtg79692 | — | W2C: Multicast traffic duplicated when OIR card comes back up |
| CSCee55603 | Infrastructure | SNMP ACL does not work for VRF interfaces |
| CSCee83031 | Infrastructure | test crash, dumping log before command is displayed |
| CSCek77907 | Infrastructure | show  run partition does not work with  vrf aware ospf process |
| CSCin66315 | Infrastructure | Inconsistency with sysuptime and rttMonLatestRttOperTime |
| CSCin89580 | Infrastructure | Incorrect entry returned by SNMP query in CAT6k platform |
| CSCsd55997 | Infrastructure | archive tar /xtract prematurely stops unpacking files if target is LEFS |
| CSCse97095 | Infrastructure | C2W1: int range po shows it can allow upto 445 ports against 256 max |
| CSCsh64390 | Infrastructure | SNMP Proxy Get-Next fails when called with a single OID. |
| CSCsk85192 | Infrastructure | copy command with : after attribute is not checked against ACS. . |
| CSCsl52962 | Infrastructure | interface range Port-channel command causes RP crash |
| CSCsm95041 | Infrastructure | Write command causes SBY RP to crash if 2nd user viewing startup config |
| CSCso40612 | Infrastructure | 7600 HA router crashed @ parser_syntax_cleanup on |

| Identifier | Technology | Description |
|---|---|---|
| CSCsv81952 | Infrastructure | CLI Views: Standby Reloads after creating view or Superview |
| CSCsx10028 | Infrastructure | Core dump may fail to write |
| CSCsx27136 | Infrastructure | carson ION:  crashinfo from Dome drops last character/line |
| CSCsy24505 | Infrastructure | Process "sbin/dfs_disk0.proc" crashed while inserting CF @ dfs_id_delete |
| CSCsy46543 | Infrastructure | HTTP command "default interface" reboots WS-X4503+ SUP in red. mode. |
| CSCsy94827 | Infrastructure | Support for ":" Illegal character should be removed |
| CSCsz09775 | Infrastructure | Routers may fail to create crashinfo due to mallocfail in mem corruption |
| CSCsz29272 | Infrastructure | Crash issuing commands on SP after SCP transfer |
| CSCsz38328 | Infrastructure | DDNS HTTP packet has ip address instead of FQDN in 'Host' field |
| CSCta18073 | Infrastructure | Memory leak in "IP SLAs Event Pr" |
| CSCtb37662 | Infrastructure | Deferencing a null ptr in syncNlmLogTableVarbind_callback leads to crash |
| CSCtb40985 | Infrastructure | IP SLA memory leak with invalid source address |
| CSCtb47647 | Infrastructure | Active RP crashed at pim_send_join_prune |
| CSCtb59930 | Infrastructure | Tacacs+ rem_addr field not sent in HTTP authentications |
| CSCtc21712 | Infrastructure | TE-RFC-MIB:mplsTunnelPerfHCPackets/Bytes show incorr value |
| CSCtc43231 | Infrastructure | SNMP Informs Source Interface Command not working |
| CSCtc61794 | Infrastructure | ISSU/SSO upgrade fails with "logging discriminator" commands |
| CSCtc86476 | Infrastructure | Cannot set value for rttMonEchoAdminCodecPayload greater than 1500 |
| CSCtc87480 | Infrastructure | dir slavenvram and wr mem triggers slavenvram:/(Device or resource busy) |
| CSCtd62220 | Infrastructure | %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, |
| CSCte52416 | Infrastructure | VSS member switch crash when power down active switch |
| CSCte79777 | Infrastructure | Syslog with filter: Process hog by Logger and crash |
| CSCtf04954 | Infrastructure | Depracate cns config notify diff on pre-component code |
| CSCec19891 | IPServices | DHCP client needs automatic route to DHCP server via default gateway |
| CSCeg27235 | IPServices | DHCP: BOOTP sends RENEW request which causes problems |
| CSCsa47672 | IPServices | NAT refcount counter maximum value of 65536 (64K) |
| CSCsc35536 | IPServices | memory leak when no serivce dhcp/service dhcp |
| CSCse01431 | IPServices | NAT-CCE : NAT SBC : outside sip call not go through |
| CSCse59109 | IPServices | high CPU usage when IP SLA is enabled |
| CSCse70141 | IPServices | Tracebacks @ ipnat_nbss_is_special_packet |
| CSCse72665 | IPServices | Mem leak at ipnat_remove_static_cfg and ipnat_add_static_cfg |
| CSCsg89055 | IPServices | Traceback due to NBSS pak parsing during IMBlock PhaseII testing |
| CSCsi93916 | IPServices | Alignment Error/ Traceback @ ipnat_nbss_is_special_packet/ latest SPUD |
| CSCsj19805 | IPServices | ip igmp static-group broken after reload on int vlan on a 7600 |
| CSCsl76411 | IPServices | IOS FTP client does not support multi-line replies |
| CSCso06542 | IPServices | NAT VRF command gets corrupted in running  config |
| CSCsy24878 | IPServices | DHCPv6 relay CLI allows any int for output causing severe problems |

| Identifier | Technology | Description |
|---|---|---|
| CSCsz51146 | IPServices | TCP bad segment and sequence number in BGP raises CPU on SXI1 modular |
| CSCsz56393 | IPServices | Modular IOS - SUP720 - Sends malformed syslog packet |
| CSCsz72591 | IPServices | Router configured as a DHCP client crashes with crafted DHCP packet. |
| CSCsz91851 | IPServices | NAT : ESP packets not translated with static NAT outside translation |
| CSCsz97239 | IPServices | PmtuAger Expiration and MSS value |
| CSCta08194 | IPServices | Router crashes when reprovisioning AToM tunnel |
| CSCta10764 | IPServices | uSBC RLS4:SBC SIP no vrf aware when overlapping address |
| CSCta23301 | IPServices | FTP: ctrl and data conn do not get terminated when cp'n 0 byte fileftp |
| CSCta55610 | IPServices | ISSU(MCPDEV->RLS3X):Stby failed to come up after R1 reload |
| CSCta56667 | IPServices | tcp.proc displays excessive cpu usage |
| CSCta77091 | IPServices | "socket SO_UDPCHECKSUM option setting failed" when sla responder |
| CSCta83548 | IPServices | NAT Platform: unable to clear an specific nat entry |
| CSCta89283 | IPServices | Add support for NAT redundancy feature in SX releases |
| CSCta97782 | IPServices | delay reload timer incorrectly start when standby changing to active 1st |
| CSCtb58282 | IPServices | show tcp brief can cause crash |
| CSCtb72550 | IPServices | Call Detail Record File not created in FTP Server |
| CSCtc17163 | IPServices | rsh command does not honor enable setting |
| CSCtc18841 | IPServices | arp entry becomes incomplete state with local-proxy-arp |
| CSCtc22729 | IPServices | proxy-arp inconsistent with HSRP ipv4 and GLBP ipv6 in 122-33.SXI |
| CSCtc55616 | IPServices | RSA key generation from SSH session disables SSH service in ION |
| CSCtc60424 | IPServices | EBGP Neighbor send to another port for FIN packet |
| CSCtd13820 | IPServices | Show Standby causes unexpected exception to CPU: crash at standby_show |
| CSCtd13999 | IPServices | Bugs in the Path-mtu logic |
| CSCtd16493 | IPServices | port xx in use by system error while configuring NAT |
| CSCtd21890 | IPServices | Router crash at dhcp autoinstall |
| CSCtd32285 | IPServices | No nat translation with PAT applied  on VRF interfaces |
| CSCtd46206 | IPServices | After Reload NAT does not create dynamic aliases and arp entry. |
| CSCtd60670 | IPServices | Username not included in the SNMP trap when tacacs authentication used |
| CSCtf21937 | IPServices | UDP Modular IOS sends out DHCP Packet with diff source-IP comp. to IOS |
| CSCtf34691 | IPServices | HSRP group name tied to static NAT for redundancy is not saved to config |
| CSCsc62963 | LAN | Have configurable MTU Range 1500 -1530 on PA-1FE and PA-2FE |
| CSCtd47338 | LegacyProtocols | DLSw generates corrupted internal router UDP pakets |
| CSCte78230 | LegacyProtocols | DLSw Ethernet Redundancy and IPV6 will not work together |
| CSCta48816 | Management | CDP Protocol: %SYS-2-GETBUF: Bad getbuffer, bytes= 32717 |
| CSCtc40711 | Management | next-hop verify-availability still forwards traffic with no CDP neighbor |
| CSCtc45716 | Management | SNMPWALK of ipRouteEntry.7 with a view configured triggers high CPU |
| CSCtd43540 | Management | Memory leak at cdp_handle_version_info |

| Identifier | Technology | Description |
|---|---|---|
| CSCej82248 | MPLS | %LFD-3-NOOCE: Traceback in lfd_fib_update_mpls_oces |
| CSCta32836 | MPLS | Vrf is not getting deleted and stuck in this state (backout CSCsx74883) |
| CSCtb13472 | MPLS | asr1:ldp:core session also flaps on flappping emulated ldp sessions. |
| CSCtb17388 | MPLS | cmfi_vpnid_is_valid Invalid Vpn Id: messages while cfiging large# of vpn |
| CSCtc90579 | MPLS | Block allocated by 'rsvp_hc_db_nbr_alloc' gets corrupted |
| CSCte56840 | MPLS | Auto-bw collect timer maxed out |
| CSCsm13783 | Multicast | No (*, G) join received from CE1 on PE1 MVPN |
| CSCsz47622 | Multicast | Traceback seen at default_ip_raw_enqueue while testing gnat-vif |
| CSCta01025 | Multicast | Inconsistent multicast MIB output compared to show ipmroute |
| CSCtb76828 | Multicast | %SYS-2-BADSHARE: Bad refcount in datagram_done for MSDP process |
| CSCtc43521 | Multicast | During soft link recovery, PIM flaps seen with other PIM neighbors |
| CSCtf11034 | Multicast | PIM Join/Prune with RP-bit set is not NATed |
| CSCtf34720 | Multicast | DR will not send periodic join for SSM group with "static-group" config |
| CSCdj40945 | PPP | PPP multilink MRRU value is not configurable |
| CSCsi49953 | QoS | sip1- tx cpu crashes @ blt_pak_holdq_peek with RCK070410 |
| CSCsl70963 | QoS | Priority and class default pkts drop-H/W MLP+fragment+llq on SIP400 |
| CSCta26106 | QoS | RSVP-3-CONSISTENCY error followed by an unexpected reboot. |
| CSCdp10763 | Routing | EIGRP:(12.0S only)Once manual summary Admin Distance set, cannot chg |
| CSCdz75312 | Routing | EIGRP does not work when seq number becomes negative |
| CSCek27981 | Routing | NRT:dn6 script fails due to timing issue. . |
| CSCsa86801 | Routing | Traceback messages seen at ipigrp2_route_map_inform. |
| CSCsd14873 | Routing | Allow Multiple EIGRP Processes To Use the Same RID on One Router |
| CSCsd78551 | Routing | EIGRP internal route tag is not carried across PE routers |
| CSCse25308 | Routing | EIGRP Neighbor relationships are torn down after changing the MTU Size |
| CSCsi46522 | Routing | During ciscoEigrpMIB access ,Spurious memory access made @ mib_get_intf |
| CSCsk47893 | Routing | eigrp stub function doesn't work correctly |
| CSCsk92412 | Routing | EIGRP:PE-CE:HopCnt/SoO attrs skipped when redist w/metric on route-map |
| CSCsl65407 | Routing | EGIRP SOO: Routing loop occurs when modifying EIGRP metrics on CE-PE i/f |
| CSCsl76135 | Routing | Tracebacks seen when eigrp neighbour goes down. |
| CSCsm14899 | Routing | ip nhrp cache non-authoritative command should not be hidden |
| CSCsm25000 | Routing | IPv6 Route not removed from routing table: metric == infinity |
| CSCsm62215 | Routing | Bus error crash with NHRP |
| CSCsm79085 | Routing | EIGRP routes flapping due to nexthop changed |
| CSCsm95129 | Routing | "no ip next-hop-self eigrp" not working when redistribute from BGP |
| CSCso56038 | Routing | %DUAL-3-INTERNAL traceback at igrp2_packet_community_add_item |
| CSCso98964 | Routing | EIGRP authentication not working for long key-strings |
| CSCsr49376 | Routing | Switch crash at eigrp_ipv4_rib_rdbupdate |

| Identifier | Technology | Description |
|---|---|---|
| CSCsr51164 | Routing | distribute-list command conversion to use parser db |
| CSCsr82785 | Routing | APS Failover of large # of interfaces takes a long time |
| CSCsu25206 | Routing | EIGRP tag-based filtering broken if tag is changed on the fly |
| CSCsu78975 | Routing | Crash seen @adj_switch_ipv4_generic_les on 38xx router |
| CSCsv56081 | Routing | ACE sequence numbers changed after the 2nd switchover |
| CSCsv66694 | Routing | EIGRP:tag not set correctly from BGP community info |
| CSCsv77932 | Routing | Router crash while configuring serial int for insufficient mtu |
| CSCsw22106 | Routing | Switch crash at eigrp_ipv4_rib_rdbupdate continuation of CSCsr49376 |
| CSCsw42724 | Routing | EIGRP: cant reach SSO terminal state with distribute-list in VRF context |
| CSCsw80640 | Routing | %SYS-2-SHARED errors when forwarding UDP packets |
| CSCsw91250 | Routing | IP-EIGRP(0) 100: Internal Error,  -Traceback@dual_packetize_interface |
| CSCsx18270 | Routing | EIGRP: tags from version 2 peers are not displayed in topology table |
| CSCsx20147 | Routing | Incorrect metric calculation for EIGRP for IPv6 |
| CSCsx42982 | Routing | EIGRP query is sent to stub peers when MD5 authentication is enabled |
| CSCsx70561 | Routing | IOS will retain the  community-list name even after unconfig |
| CSCsx75866 | Routing | EIGRP Stub-Site:  routing loop when poison suppressed |
| CSCsy42615 | Routing | Entries missing from OSPF router route table |
| CSCsy56736 | Routing | SIP-200 crash with "ip rtp-header compression format ietf" in MLPPP |
| CSCsz36368 | Routing | EIGRP extended community synchronisation issue |
| CSCsz43096 | Routing | Getting mismatch pkts in show ip cache verbose flow,com. to expected one |
| CSCsz53614 | Routing | Incorrect notification sent to OSPF when subinterface added |
| CSCsz76616 | Routing | PPP negotiation does not happening |
| CSCta05516 | Routing | EIGRP offset-list does not rescan when ACL is modified |
| CSCta07104 | Routing | Config-Sync & Traffic failure in VPN SSO scripts |
| CSCta19718 | Routing | %SCHED-3-STUCKTMR: Sleep with expired timer |
| CSCta46880 | Routing | Directly connected IP adress is learnt via ISIS, "clear ip rou" fixes. |
| CSCta60119 | Routing | non recursive accounting can cause prefixes linked to drop |
| CSCta79313 | Routing | Traceback seen when modifying route-map associated with BGPredistributio |
| CSCta93223 | Routing | Router crashed upon confuguring ip extcommunity and issuing show run |
| CSCta99162 | Routing | Switch reloads when entering the command passive-interface default |
| CSCtb01505 | Routing | Router crashes with ospf_build_net_lsa |
| CSCtb01934 | Routing | sh ip bgp vpnv4 vrf <VRF> x.x.x.x longer/shorter commands do not work. |
| CSCtb35914 | Routing | nsf command not available in non-modular IPBase image. |
| CSCtb36384 | Routing | ipdatastart_iph() could cause problem when called from interrupt path |
| CSCtb37132 | Routing | OSPF NSF processing fails on iprouting process restart |
| CSCtb38882 | Routing | OSPF-MIB returns only one OSPF process 12.2SX |
| CSCtb43448 | Routing | EIGRP:interf cmds not removed from Standby conf when deleted from Active |

| Identifier | Technology | Description |
|---|---|---|
| CSCtb70508 | Routing | OSPF Summary route not advertised after convegence/flaps from CE to PE |
| CSCtb82674 | Routing | IS-IS adjacency stays down after switchover |
| CSCtb91412 | Routing | Ipv6/named-mode/Eigrp session goes down if one of ipv6 addr is deleted |
| CSCtb94723 | Routing | 31SB16:RR sending illegal pfx in withdraw to old style MDT PE |
| CSCtc01196 | Routing | Carson: ISIS topology broken after 2-3 consecutive SSO |
| CSCtc31545 | Routing | EIGRP - Active routes remain in topo table after link flap |
| CSCtc36727 | Routing | ospfNbrIpAddr unnumbered interface entries don't include the neighbor IP |
| CSCtc39809 | Routing | Memory leak @ dual_sia_active |
| CSCtc57092 | Routing | Standby resets due to MCL issue with offset-list name inconsistency |
| CSCtc59162 | Routing | EIGRP resync is not triggered when modifying inbound/outboun prefix-list |
| CSCtc70737 | Routing | Static routes are not in EIGRP topo table after add/remove the static |
| CSCtc72772 | Routing | Bulk sync failure and Standby reloads continuously @ "clns route" |
| CSCtc73440 | Routing | Changing interface ip address/mask triggers a bad OSPF route |
| CSCtd00479 | Routing | ISIS IETF NSF fails on LAN interface when restarting router is a DIS |
| CSCtd07257 | Routing | OSPF does not remove unnecessary redistributed routes |
| CSCtd42462 | Routing | Show CLNS traffic command output showing negative values. |
| CSCtd48455 | Routing | Summary and components seen after 'clear ip route' w/ ip summary-address |
| CSCtd49246 | Routing | round-trip average of ping MIB may show less value |
| CSCtd68197 | Routing | mem leak in IPv6 RIB Redistribute with EIGRP Work Ent |
| CSCtd73256 | Routing | a catalyst switch may reload unexpectedly during 'show ip ospf int' |
| CSCtd73951 | Routing | OSPF discard-route(Null0) is deleted when area auth command is removed |
| CSCtd86572 | Routing | DMVPN EIGRP next hop update not sent to spoke |
| CSCte10790 | Routing | c6500: device crashing on removing ace entry or entire acl |
| CSCte29212 | Routing | EIGRP summary leak-map is not independent of AD keyword |
| CSCte39250 | Routing | Router crashes @ ipv6_show_interface |
| CSCte53365 | Routing | Connected global address not in eigrp topo after 'no shut' v6 process |
| CSCte54840 | Routing | Router crashed at ospfv3_routerid_command during simultanious operation |
| CSCte54852 | Routing | Route of non-first interfaces on Secondary Module is added later |
| CSCte57710 | Routing | Process replies to ping to I/F downed unlike cef handling. |
| CSCte58468 | Routing | OSPF conditional default route not advertised after config removed |
| CSCte58962 | Routing | Line-by-Line sync verifying failure after "no router ospf" command |
| CSCte69761 | Routing | Default Route deleted when prefix marked as candidate default is deleted |
| CSCte73093 | Routing | distribute-list with an explicit interface does not work. |
| CSCte91997 | Routing | DHCP breaking when DHCP server and VRRP master are same. |
| CSCtf06436 | Routing | high CPU due to HW backwalk continually walking the looped OCE chain |
| CSCtf16300 | Routing | clear arp-cache is not working correctly |
| CSCtf45374 | Routing | Eigrp route-tags not sent using distribute-list |

| Identifier | Technology | Description |
|---|---|---|
| CSCei66915 | Security | Incorrect option for ip-address under crypto pki |
| CSCsb10291 | Security | $$TS: Router forced crash on PKI Bind service failure (C_UnbindService) |
| CSCsd84640 | Security | SSH2 Error message should adhere to Cisco Syslog Format |
| CSCsd98525 | Security | SSH2 session closes prematurely |
| CSCse31829 | Security | Memory leak in Crypto IKMP process |
| CSCsf17411 | Security | trustpoint authentication fails if key usage is non standard |
| CSCsg75994 | Security | Show login failure output does not display Username |
| CSCsk05015 | Security | USERAUTH_SUCCESS not handled correctly for "none" auth method |
| CSCsl02104 | Security | SSH Unexpected mesg type received should display in Cisco Syslog Format |
| CSCsl10459 | Security | show crypto pki timers command causes a software forced crash |
| CSCso27236 | Security | IOS CA client shows renew date 1 Jan 1970 |
| CSCsu29044 | Security | Inconsistencies attaching policies to Tunnel and physical interfaces |
| CSCsv54863 | Security | IOS PKI: Not expired Certificate is deleted if autoenrollment fails |
| CSCsv92274 | Security | SSH process might not handle some IPC messages |
| CSCsx17447 | Security | IOS not including HOST header in HTTP CRL request |
| CSCsz83570 | Security | SSH Sessions disconnect when viewing logs w/ pagers |
| CSCsz84055 | Security | System crashed unexpected while open ssh2 session |
| CSCsz92328 | Security | Some configs not synced with crypto certificate configured on active |
| CSCta77073 | Security | Router Crash while unconfiguring crypto trustpoint |
| CSCtc12312 | Security | PKI may get stuck after 32678 CRL fetches |
| CSCtc41114 | Security | New SSH sessions with RSA key fails after changing hostname |
| CSCtd35586 | Security | Tunnel on VRF bring down due to HSRP status change on Non VRF |
| CSCtd78270 | Security | 12.2 : ssh feature needed to allow selection of rsa keys to use |
| CSCtf47512 | Security | SXH5: Memory leak in ACE HAPI and IPSec Key Engine |
| CSCsw31019 | WAN | Router crashes while configuring the command "frame-relay be 1" |
| CSCtd22993 | WAN | SNMP ifIndex for certain serial interfaces becomes inactive |

## Caveats Resolved in Release 12.2(33)SXI3

### Resolved MPLS Caveats

- CSCsz45567—Resolved in 12.2(33)SXI3

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

#### Resolved Unknown Caveats

- CSCtc41760—Resolved in 12.2(33)SXI3

  **Symptom:** 6500 may experience redzone crash at UDLD process. Message may appear %SYS-SP-3-OVERRUN: Block overrun at 44456570 (red zone 6D000700) -Traceback= 40291448 402938DC 40D74570 40D763A0

  Traceback will vary from code to code.

  **Conditions:** UDLD configured

  **Workaround:** Disable UDLD.

- CSCsh61458—Resolved in 12.2(33)SXI3

  **Symptoms:** A Cat4k switch may reload after receiving a malformed packet on one specific specific port.

  **Conditions:** This symptom may be observed on a Cat4k switch that enables DNSIX audit trail and recieves crafted IP packets on a specific port.

  **Workaround:** Do not enable the DNSIX audit trail.

#### Other Resolved Caveats in Release 12.2(33)SXI3

| Identifier | Technology | Description |
|---|---|---|
| CSCei37916 | AAA | Incorrect AAA behavior when both wait-accnt & broadcast accnt is con |
| CSCsc97727 | AAA | Access Point Crashes When Removing TACACS Server |
| CSCsq71492 | AAA | IOS device crash or tracebacks at tplus_handle_req_timeout |
| CSCsy55362 | AAA | Unresponsive Console/VTYs |
| CSCse75697 | ATM | LOKI: ima clock should default to LINE, backout CSCin90422, CSCsb68536 . |
| CSCej00344 | — | Crash when opening new session from router |
| CSCek53099 | — | SIP200+4xT3/E3:Fail to load cRTP CFG from startup file |
| CSCsb88996 | — | slb traceback spurious memory access after slb statefull switchover |
| CSCsk88751 | — | Kron CLI Process 'show tech-support password |
| CSCso35876 | — | SRB3:New active SP crash at label_entry_get_inlabel |
| CSCso36150 | — | duplicate vlan names causing config-sync failures |
| CSCso79135 | — | Wism controller ports 1 state is down after mod shut/unshut |
| CSCso79925 | — | EC with enhanced hash method (PFC3C) has no knob to use old method (3B) |
| CSCsr04916 | — | PBR dropped the packets after add set vrf vpn1 back to the route-map |
| CSCsr99518 | — | Granikos should not init rekey after recieving new outbound SA at QM3 |
| CSCsu29301 | — | C2W21: Ingress SPAN on Sup - ACE module duplicates packets |
| CSCsu67413 | — | RRI - Route disappears after ipsec rekey with multi int scenario |
| CSCsu81976 | — | IPSEC NAT traversal fails to correctly track SAs |
| CSCsu84213 | — | RPF-MFD hardware entry is missed after doing SSO. |

| Identifier | Technology | Description |
|---|---|---|
| CSCsv27372 | — | telnet to a real(directed mode) via GRE tunnel crates SUP crash on SRC2 |
| CSCsw28024 | — | Router is getting crashed at crypto_ikmp_cfg_auto_update_parameters |
| CSCsx13442 | — | After shut no shut hub tunnel, spoke cannot trigger isakmp SA |
| CSCsx81468 | — | CWPA2: Drops CLNS Hello packets |
| CSCsy03587 | — | c2w2b: SYS-2-MALLOCFAIL: Memory allocation  failed seen with tracebacks |
| CSCsy07709 | — | C2W2: %COMMON_FIB-4-FIBNULLIDB: Missing idb for fibidb Port-channel5A |
| CSCsy30937 | — | Modify dual-active fast-hello function for rapid detection and recovery. |
| CSCsy34566 | — | Disable VLAN mapping on ME6524, 6148A-GE-TX |
| CSCsy69740 | — | SXH: Traffic drop on L2 PO after cleared psecurity on rcving L2 ports |
| CSCsz01976 | — | Need a cli to dump the rommon environment and unset rommon variable |
| CSCsz04297 | — | Cat6k: False Dynamic MAC entry is installed with format 0000.<LTL>.0000 |
| CSCsz23445 | — | %PORT_SECURITY-SP-6-INVALID_SESSION: Invalid Port-Security ISSU Session |
| CSCsz36826 | — | 6509E fan-tray failed to restore back to HP mode after OIR |
| CSCsz50968 | — | ace interface and vlans up but has no ip connectivity to CAT 6K |
| CSCsz74896 | — | VSS redundancy reload shelf X causes UDLD err-disable |
| CSCsz76015 | — | C2W2: Need cli to set PF_BIAS to ensure lower slot# Sup boots as active |
| CSCsz81520 | — | MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC: RP failed allocating IPC buffer |
| CSCsz81627 | — | spurious memory accesses due to snmp |
| CSCsz83701 | — | W2B: SFP-UTP entPhysicalVendorType cevSFP1000BaseSx to zeroDotZero |
| CSCsz84544 | — | output drops increment on not-connected interface of 6548GE-TX module |
| CSCsz86787 | — | IPV6 mcast and IPV4 EMVPN VRF Lite traffic are not forwarded after SSO |
| CSCsz87648 | — | SP/RP and redundant system handshake broken when the kernel crashes. |
| CSCsz92137 | — | Crash in crypto_destroy_sadb_root() upon unconfiguring tunnel protection |
| CSCsz92508 | — | SPA module reloads when no response to keep-alive polling |
| CSCsz96469 | — | Tracebacks seen @chunk_free_with_pc while unconfiguring |
| CSCta06175 | — | Cat6500/SXH: Deleted configs re-appear on IDSM reset |
| CSCta06689 | — | Rapid PVST:mac address table not flushed after topology change |
| CSCta10402 | — | Tracebacks seen due to BFD PP Process |
| CSCta10870 | — | FPOE takes long time to be programmed on active vss switch |
| CSCta14457 | — | A Cisco device may report alignment errors |
| CSCta15415 | — | DHCP Snooping functionality is not working fine with private vlan |
| CSCta15851 | — | Changing allowed vlan mask causes WiSM LAG member ports to reset |
| CSCta17587 | — | VRF + RHI combination does not work on FWSM |
| CSCta21771 | — | %CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at  0 error on modul |
| CSCta22749 | — | C2W2b: %CONST_DIAG-SW1_SP-3-BOOTUP_TEST_FAIL:LC powercyled during Multip |
| CSCta27279 | — | WCCP s/w switching with Ingress redirection & interface ACL |
| CSCta30298 | — | CHKPT-SP-3-NOMEM: Memory leak seen and later the box crashed |

| Identifier | Technology | Description |
|---|---|---|
| CSCta32922 | — | SP crash due to heartbeat failure. |
| CSCta36799 | — | Router Crases @ ppcp_ppm_add_class_to_stored_policy_internal |
| CSCta36939 | — | c2w2b:Crash On ISSU Run Version |
| CSCta42989 | — | "%CSM parser state"  configuring CLI when configuring via XML also |
| CSCta44166 | — | Memory leak seen with dynamic crypto map |
| CSCta48968 | — | Modular IOS kernel crashinfo has missing information |
| CSCta52689 | — | cat6k crash in RP due to address error with wccp configuration |
| CSCta55498 | — | [Modular IOS] MIPS CP0 registers save algorthim needs a few improvements |
| CSCta56676 | — | IPsec SA liftime can go to negative values |
| CSCta57705 | — | C2W2b: reg_invoke_vs_ltl_src_index_changed() needs to be added on stdby. |
| CSCta57778 | — | auth-mgr/eap::  %IDMGR-3-INVALID_ID: bad id in id_get (bad table id) |
| CSCta60531 | — | VSS Preemption causes CAM table updation fails in FWSM env |
| CSCta67007 | — | c2hd1:VRF interfaces not shown and not pinging the CE's |
| CSCta68053 | — | time-period does not take effect in configuration archive |
| CSCta74242 | — | VSS: crash due to snmp get after standby chassis reloads |
| CSCta74315 | — | WS-X6324-100FX-MM May Be Inoperable and Have Status "Other" |
| CSCta84749 | — | Etherchannel should not be allowed if auto qos is enable |
| CSCta94179 | — | Recirculated MPLS packets becasue of egress service policy are dropped |
| CSCtb03003 | — | MAC table on standby Supervisor not flushed on link change |
| CSCtb15569 | — | VPN-SPA - traffic failed to decrypt due to SecInfo check failure |
| CSCtb23289 | — | Major temperature alarm has to force system shutdown |
| CSCtb27643 | — | cat6000 Medium buffers leak on SP leading to crash |
| CSCtb38547 | — | Incorrect CP0 values and empty kernel variable section in kernel crashin |
| CSCtb62523 | — | PfR - inside prefixes not learned on cat6k BR |
| CSCtb63352 | — | VSS: With 6KW DC PS, no power to bringup VSL supervisor or linecard |
| CSCtb66983 | — | Nas-port-type is missing in Access-request |
| CSCtb68478 | — | "Illegal nextSsIndex value" message should be removed |
| CSCtb83677 | — | Power Deny for pre-standard power on SXI2 or Later |
| CSCtb87454 | — | DHCP Rogue Server Detection |
| CSCee83031 | Infrastructure | test crash, dumping log before command is displayed |
| CSCsd99763 | Infrastructure | Cisco 7200 series reload unexpectedly while configuring BGP acces list |
| CSCsu65967 | Infrastructure | Modular IOS crash at free_lite_internal |
| CSCsv30540 | Infrastructure | Memory corruption in remove_ws when NULL string is passed |
| CSCsx10028 | Infrastructure | Core dump may fail to write |
| CSCsy24505 | Infrastructure | Process "sbin/dfs_disk0.proc" crashed while inserting CF @ dfs_id_delete |
| CSCsy31159 | Infrastructure | ASR1k 'show history all' is NOT updated properly |
| CSCsy88640 | Infrastructure | nested crash in crashinfo collection. |

| Identifier | Technology | Description |
|---|---|---|
| CSCsz29272 | Infrastructure | Crash issuing commands on SP after SCP transfer |
| CSCta02715 | Infrastructure | SXH5: RP crash on each booting time if <logging count> enabled |
| CSCtb37662 | Infrastructure | Deferencing a null ptr in syncNlmLogTableVarbind_callback leads to crash |
| CSCsi99841 | IPServices | vrf-aware trustpoint authentication/enrollment doesn't work |
| CSCsj19805 | IPServices | ip igmp static-group broken after reload on int vlan on a 7600 |
| CSCso06542 | IPServices | NAT VRF command gets corrupted in running config |
| CSCsw65614 | IPServices | NAT with route maps doesn't work for TCP application |
| CSCsz51146 | IPServices | TCP bad segment and sequence number in BGP raises CPU on SXI1 modular |
| CSCsz89107 | IPServices | high cpu due to ip_input process during SNMP trap |
| CSCta24043 | IPServices | "%IPNAT-4-ADDR_ALLOC_FAIL" message seen when all ports are not allocated |
| CSCta27331 | IPServices | HSRP authentication applied to secondary addresses fails |
| CSCta77091 | IPServices | "socket SO_UDPCHECKSUM option setting failed" when sla responder |
| CSCta83548 | IPServices | NAT Platform: unable to clear an specific nat entry |
| CSCta89283 | IPServices | Add support for NAT redundancy feature in SX releases |
| CSCtb58282 | IPServices | show tcp brief can cause crash |
| CSCsz05918 | Management | CDP neighbors do not come up on vlan interface |
| CSCsz75221 | Management | A local variable in cdp takes up 2k process stack space-prompting crash |
| CSCej82248 | MPLS | %LFD-3-NOOCE: Traceback in lfd_fib_update_mpls_oces |
| CSCsx82365 | MPLS | LDP does not immediately send all IP addresses on new session |
| CSCsz75180 | MPLS | Crash due to mpls subintf being removed |
| CSCsz92368 | MPLS | MDEBUG-2-ACCESSFREED: @tc_handle_dead_peers Enabling/disabling "mpls ip" |
| CSCta32836 | MPLS | Vrf is not getting deleted and stuck in this state (backout CSCsx74883) |
| CSCsm13783 | Multicast | No (*, G) join received from CE1 on PE1 MVPN |
| CSCsz63723 | Multicast | [UNI] MLD entry denied by mCAC isn't deleted. |
| CSCsz88850 | Multicast | Rework CSCsz16580 fix |
| CSCta26106 | QoS | RSVP-3-CONSISTENCY error followed by an unexpected reboot. |
| CSCsm57831 | Routing | EIGRP: admin tags do not propagate between eigrp peers |
| CSCsm79085 | Routing | EIGRP routes flapping due to nexthop changed |
| CSCsq83006 | Routing | Port-channel down makes EIGRP SIA |
| CSCsu78975 | Routing | Crash seen @adj_switch_ipv4_generic_les on 38xx router |
| CSCsw16157 | Routing | Crash following OSPF and MPLS-TE tunnel changes |
| CSCsw42724 | Routing | EIGRP: cant reach SSO terminal state with distribute-list in VRF context |
| CSCsz31770 | Routing | Per-user static route is not installed on LNS after session established |
| CSCsz43096 | Routing | Getting mismatch pkts in show ip cache verbose flow,com. to expected one |
| CSCsz76701 | Routing | Supervisor crash with decodeds pointing to ISIS |
| CSCsz84906 | Routing | isis redistributed route is not removed when interface shutsdown |
| CSCta08632 | Routing | ISIS topology broken after Sup force-switchover with ispf |

| Identifier | Technology | Description |
|---|---|---|
| CSCta60119 | Routing | non recursive accounting can cause prefixes linked to drop |
| CSCta93223 | Routing | Router crashed upon confuguring ip extcommunity and issuing show run |
| CSCta99162 | Routing | Switch reloads when entering the command passive-interface default |
| CSCtb01505 | Routing | Router crashes with ospf_build_net_lsa |
| CSCtb35914 | Routing | nsf command not available in non-modular IPBase image. |
| CSCtb43448 | Routing | EIGRP:interf cmds not removed from Standby conf when deleted from Active |
| CSCsc49862 | Security | IPaddress in Subject Alternative Name is not parsed correctly. |
| CSCso27236 | Security | IOS CA client shows renew date 1 Jan 1970 |
| CSCsv54863 | Security | IOS PKI: Not expired Certificate is deleted if autoenrollment fails |
| CSCsy74318 | Security | aaa authentication fail-message not displayed over SSH |
| CSCsz84055 | Security | System crashed unexpected while open ssh2 session |

## Caveats Resolved in Release 12.2(33)SXI2a

| Identifier | Technology | Description |
|---|---|---|
| CSCsu65967 | Infrastructure | Modular IOS crash at free_lite_internal |
| CSCtb15569 | — | VPN-SPA - traffic failed to decrypt due to SecInfo check failure |
| CSCtb27643 | — | cat6000 Medium buffers leak on SP leading to crash |

## Caveats Resolved in Release 12.2(33)SXI2

### Resolved Infrastructure Caveats

- CSCsx49573—Resolved in 12.2(33)SXI2

  **Symptom:** Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http

  **Conditions:** See “Additional Information” section in the posted response for further details.

  **Workarounds:** See “Workaround” section in the posted response for further details.

### Resolved IPServices Caveats

- CSCsv87997—Resolved in 12.2(33)SXI2

  **Symptom:** DHCPv6 relay process crash on Actice RP.

  **Conditions:** Unknown at this time.

  **Workaround:** Unknown at this time.

- CSCsw18636—Resolved in 12.2(33)SXI2

  **Symptoms:** High CPU utilization occurs after device receives a ARP packet with protocol type as 0x1000.

**Conditions:** This problem occurs on Supervisor 32 running Cisco IOS Release 12.2(33)SXI. This problem may also occur on Supervisor 720. The problem is only seen when you have bridge-group CLI being used, which leads to ARP packets with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

**Workaround:** Filter the ARP packet. The device configuration should have bridge-group creation first, followed by interface-specific bridge-group options.

- CSCsx16152—Resolved in 12.2(33)SXI2

  **Symptom:** Under unique circumstances erroneous routing prefixes may be added to the routing table.

  **Conditions:** When the DHCPv6 relay feature is enabled and a router receives a normal DHCPv6 relay reply packet, this may lead to an erroneous route being added to the routing table.

  **Workaround:** No workaround except turning off DHCPv6 relay.

#### Resolved MPLS Caveats

- CSCsz45567—Resolved in 12.2(33)SXI2

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

#### Resolved Multicast Caveats

- CSCsm64082—Resolved in 12.2(33)SXI2

  **Symptom:** The router may report AUTORP-4-PAK_ERR.

  **Conditions:** PIM Auto-RP is configured and ip multicast boundary is enabled with filter-autorp option.

  **Workaround:** Configure ip multicast boundary without filter-autorp option.

#### Resolved Routing Caveats

- CSCsx73770—Resolved in 12.2(33)SXI2

  **Symptom:** A Cisco IOS device that receives a BGP update message and as a result of AS prepending needs to send an update downstream that would have over 255 AS hops will send an invalid formatted update. This update when received by a downstream BGP speaker triggers a NOTIFICATION back to the sender which results in the BGP session being reset.

  **Conditions:** This problem is seen when a Cisco IOS device receives a BGP update and due to a combination of either inbound, outbound, or both AS prepending it needs to send an update downstream that has more than 255 AS hops.

**Workaround:** The workaround is to implement **bgp maxas-limit X** on the device that after prepending would need to send an update with over 255 AS hops. Since IOS limits the route-map prepending value to 10 the most that could be added is 21 AS hops (10 on ingress, 10 on egress, and 1 for normal eBGP AS hop addition). Therefore, a conservative value to configure would be 200 to prevent this condition.

- CSCsy86021—Resolved in 12.2(33)SXI2

  Recent versions of Cisco IOS Software support RFC4893 (“BGP Support for Four-octet AS Number Space”) and contain two remote denial of service (DoS) vulnerabilities when handling specific Border Gateway Protocol (BGP) updates.

  These vulnerabilities affect only devices running Cisco IOS Software with support for four-octet AS number space (here after referred to as 4-byte AS number) and BGP routing configured.

  The first vulnerability could cause an affected device to reload when processing a BGP update that contains autonomous system (AS) path segments made up of more than one thousand autonomous systems.

  The second vulnerability could cause an affected device to reload when the affected device processes a malformed BGP update that has been crafted to trigger the issue.

  Cisco has released free software updates to address these vulnerabilities.

  No workarounds are available for the first vulnerability.

  A workaround is available for the second vulnerability.

  This advisory is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090729-bgp

#### Resolved Security Caveats

- CSCsx70889—Resolved in 12.2(33)SXI2

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels

- CSCsz32366—Resolved in 12.2(33)SXI2

  **Symptoms:** A Cisco router that is running Cisco IOS Release 12.4(25) may crash due to SSH.

  **Conditions:** This symptom occurs when SSH is enabled on the router. An attempt to access the router via SSH is made.

  **Workaround:** Do not use SSH. Disable SSH on the router by removing the RSA keys:

  “crypto key zeroize rsa”

  Further Problem Description: This issue has not been seen in Cisco IOS Release 12.4(23) and earlier releases. It also has not been seen in Cisco IOS Release 12.4T images.

#### Resolved Unknown Caveats

- CSCsy07555—Resolved in 12.2(33)SXI2

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ipsec

- CSCsy15227—Resolved in 12.2(33)SXI2

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy

- CSCsy68923—Resolved in 12.2(33)SXI2

  **Symptom:** Cisco IOS device may reload in very rare circumstances after receiving certain packets. The BFD process may restart due to a critical software exception.

  **Workarounds:** None

#### Other Resolved Caveats in Release 12.2(33)SXI2

| Identifier | Technology | Description |
|---|---|---|
| CSCei37916 | AAA | Incorrect AAA behavior when both wait-accnt & broadcast accnt is con |
| CSCei62358 | AAA | Downloading callback-dialstring as part of Tacacs+ author leads to crash |
| CSCsb34770 | AAA | AAA Authentication banner for TACACS behaviour |
| CSCse12395 | AAA | Check keys error for accounting does not cause failover |
| CSCsl63494 | AAA | Issue with session accounting in AAA |
| CSCsz07569 | AAA | Session id changes between interim and stop records |
| CSCsz43356 | AAA | CPUHOG and Traceback after multiple SSH logins |
| CSCea90968 | ATM | Bus error crash after (config-if)# atm pvp 1 |
| CSCsx43905 | ATM | Router Crash at dlcncia.c on 12.2(33.4.14)SXH |
| CSCek47612 | — | TX cpu stats not displayed in sh hw-module slot proc cpu output |
| CSCek60142 | — | FRR does not work (about 200 ms loss) with E5 SPAs,LC crash on link flap |
| CSCsd39568 | — | stats support for PBR set ip nexthop/set interface |
| CSCsd45698 | — | Cat6K: SLB punted to CPU  if src_index is port-channel index |
| CSCsg35285 | — | Slower Cache refresh for int stats when more interfaces up |
| CSCsh28072 | — | ESM may cause rotuer to crash during IPS test attack |
| CSCsi50091 | — | BFD session flaps after executing "undebug all" command. |
| CSCsj26698 | — | Acct-Session-Id in Accounting-Request is different from in Access-Reques |
| CSCsj89208 | — | RP hits TLB exception when SIP-400 OIR with 8k MPBE EFPs |
| CSCsk62032 | — | DHCP snooping support to detect rogue dhcp servers |
| CSCsl35174 | — | Setting Scorpion int MTU < packets injected results in perm 1-way traf . |
| CSCsm39160 | — | TestCFRW shows incorrectly as failed in show diagnostic sanity |
| CSCsm79995 | — | Tracebacks are seen while attaching service-policy in a atm  pvc |

| Identifier | Technology | Description |
|---|---|---|
| CSCso39162 | — | W2: SCHED-7-WATCH: Attempt to monitor... Process= "NAM_Process" & TB's |
| CSCso67500 | — | mvpn-bidir: Reloading encap rtr and performing sso causes df index issue |
| CSCso79135 | — | Wism controller ports 1 state is down after mod shut/unshut |
| CSCsq15198 | — | EPC:SRD:RSP720:OSPF/BFD flaps when Gi5/2 (RSP gi link) is no shutted |
| CSCsq69567 | — | SSO Switchover + unicast-routing chg cause MC traffic loss for 2 minutes |
| CSCsr15448 | — | C2W2: E-OAM session not established b/w CE and PE on Port mode EoMPLS |
| CSCsr43461 | — | vrf selection source < > missing under sh_run after router reload |
| CSCsr58151 | — | C2W2: EOAM:errdisabled port doesn't recover even if errdisable rcvry en |
| CSCsr59237 | — | OSPF adj flaps on WS-X6548-GETX, due to LTL / RBH programming mismatch |
| CSCsr62498 | — | C2W2: Span dest port continuously sends some traffic on 6748 cards |
| CSCsr97387 | — | Router crashed at crypto_delete_map_routes during ip address change |
| CSCsu05721 | — | C2W2: %NTI-SP-3-AGENT_ERR and TB was seen after issu runversion |
| CSCsu40166 | — | PBR packets send out to wrong next hop MAC after ACL is changed |
| CSCsu48241 | — | memory leak when removing igmp snooping with acl filtering |
| CSCsu50413 | — | RE: acl merge causes high rp cpu for ~50 min after reload |
| CSCsu52504 | — | %LINEPROTO-SP-5-UPDOWN msg is output when changing cdp configuration |
| CSCsu95857 | — | cardDescr (.1.3.6.1.4.1.9.3.6.11.1.3) is returning incorrect value |
| CSCsu99813 | — | C2HD1-SI:Span Distributed Stops Traffic - Centralized Duplicates |
| CSCsv06453 | — | Crashinfo file not created in certain cases when SP crashes. |
| CSCsv20768 | — | After SSO s/wover, atm clock config changes to line and PTB to UNSTABLE |
| CSCsv24908 | — | L2 Fwd Broken on other modules when SIP-400 int flaps |
| CSCsv27372 | — | telnet to a real(directed mode) via GRE tunnel crates SUP crash on SRC2 |
| CSCsv43187 | — | 120seconds after SSO, Some multicast traffic drops |
| CSCsv61458 | — | [no] mpls ip propagate-ttl needs no mpls ip - mpls ip to take effect. |
| CSCsv74822 | — | Crash on RPR switchover in the rf_proxy_rp_sync path |
| CSCsv79673 | — | Router MAC learned dynamically after add/remove of xconnect on SVI |
| CSCsv94560 | — | c7600/MPLS: Packet reflection over EoMPLS link when vc going up |
| CSCsv99620 | — | Some tunnels are not programmed when ipsec updates GRE in mGRE/TP |
| CSCsw14147 | — | VACL unable to capture traffic from RP |
| CSCsw21852 | — | CSM: memory leak in process "Laminar Icc Event" |
| CSCsw24172 | — | ES20:-%INTR_MGR-DFC2-3-INTR: Parsing Engine (X-Chip) [1]: Inbound Toast |
| CSCsw28972 | — | enh: provide option for port security to not install L2 trap entries |
| CSCsw31607 | — | LTL index incorrect in PI MET table |
| CSCsw38512 | — | T/B upon SSO with VSS |
| CSCsw40790 | — | SNMP Loop on PA-MC-T3+ interfaces (Installed) |
| CSCsw48824 | — | Switchport Block Unicast - prevents RTP on same VLAN |
| CSCsw49623 | — | Router crashes when PfR learn config is displayed on the border |

| Identifier | Technology | Description |
|---|---|---|
| CSCsw59517 | — | IGMPv3 snooping drops 'Block Old Sources' report |
| CSCsw68514 | — | SLB probes iin TESTing state while using client cmd in Vserver config |
| CSCsw69621 | — | BR DOWN if inside bgp is only type of learning configured |
| CSCsw76117 | — | TBs seen after redundancy mode change from sso to rpr |
| CSCsw76910 | — | IOS-SLB:Supervisor crashes on configuring/verifying firewallfarm CLIs |
| CSCsw83488 | — | Negative value seen for counters in vpn session |
| CSCsw91858 | — | Misleading error when 6716 is configured for VSL |
| CSCsw92171 | — | multiple "power-input" for new 6kW DC PS do not exist on Standby |
| CSCsw92386 | — | Not able to delete logging filter  and crash at Tcl_NewStringObj |
| CSCsw96176 | — | BFD sessions with version 0  do not come up properly following a reload |
| CSCsx06578 | — | SIERRA:MAGO switch got crashed after reload with SIERRA_INTEG_090106 |
| CSCsx07137 | — | Invalid " %FM-4-L2_DYN_TCAM_EXCEPTION" error message for some cases. |
| CSCsx09110 | — | Failed to establish ipsec tunnel with CCM |
| CSCsx09273 | — | WEBAUTH(IP adm) is not INITiating if IPDT entry already exists. |
| CSCsx10011 | — | VSS: IO memory leak from pre_process_vsibc_vsda_pak |
| CSCsx13050 | — | tcl doesn't run or Register event failed messages on Modular IOS |
| CSCsx19210 | — | [show epm session ip 0.0.0.0] crashes supervisor |
| CSCsx20081 | — | Local Web-Auth does NOT work when IP Source-Guard is enabled on port |
| CSCsx20862 | — | Peer RP index unknown messages seen on VSS setup |
| CSCsx21431 | — | Logging Filter CLI gets lost after SSO |
| CSCsx21886 | — | ISSU switchover command sync issue |
| CSCsx22711 | — | router crashes if we unconfigure 1024 GLBPv6 grp on intf and do sh mod |
| CSCsx27836 | — | VS: STP state on standby SP shows DWN sometimes and SSO causes high CPU |
| CSCsx28532 | — | VPN SPA freezes when ip mtu changed on tunnel interface |
| CSCsx29377 | — | 1 sec multicast loss on standby sup720-10g |
| CSCsx29645 | — | IPv6 Multicast traffic can not converge after SSO |
| CSCsx34570 | — | VSS:remove port-channel from interface causes other members to go down |
| CSCsx39263 | — | TCAM entries are not installed for TCP intercept after SSO |
| CSCsx46323 | — | C2W21: Standby SUP resets due to monitor session on internal PO |
| CSCsx49071 | — | After SSO on Sup4, IPV6 Multicast traffic is not forwarded |
| CSCsx49326 | — | Port-security on TenGig ports doesn't install dynamic mac as secure macs |
| CSCsx49420 | — | HQoS policy attached to main interface cannot set cos to IPv6 traffic. |
| CSCsx49718 | — | Auth Man Single-host-Guest VLAN doesn't trigger reauth on EAPOL start |
| CSCsx49889 | — | SPA-IPSEC-2G-3-ACEI0TCAMFAILE:SpdSpInstall:cannot install Sp TmInsertSp |
| CSCsx50407 | — | show authenticaiton needs to display policies for a session |
| CSCsx53964 | — | Unable to control traffic-class |
| CSCsx55152 | — | Switch does not send TC trap if it is not a root bridge |

| Identifier | Technology | Description |
|---|---|---|
| CSCsx55698 | — | auth_mgr: spurious access @ dot1x_rp_auth_client_deleted |
| CSCsx58097 | — | Tracebacks and crash @ lfd_rewrite_mgr_fill_mfi_out_info observed on SSO |
| CSCsx58488 | — | VSL interfaces are not in restricted mode |
| CSCsx58786 | — | Router crash @ routemap_track_nexthop |
| CSCsx62912 | — | W2: update the PM switch vp limits for MST, PVST and Rapid-PVST |
| CSCsx64668 | — | Config change on port of WS-X6148-FE-SFP will move other ports to down |
| CSCsx64994 | — | Memory leaks in ccm processes after redundancy forced switchover |
| CSCsx65705 | — | router crash on no route-map with match ipv6 address access-list |
| CSCsx76308 | — | HA client crashing attempting to free unassigned memory |
| CSCsx78789 | — | Router crash @ flow_sampler_select with traffic |
| CSCsx78812 | — | MLPPP+LFI over ATM : Inconsistent behavior |
| CSCsx79379 | — | IOS Auth Proxy HTTP may lead to bus error adress 0x0 |
| CSCsx82825 | — | Shutdown Loopback interfaces in VSS recovery mode |
| CSCsx83443 | — | crypto debug condition leaks messages which lead to high cpu. |
| CSCsx93160 | — | SXI image shut down linecard ports of WS-X6748-GE-TX |
| CSCsx95302 | — | C2W21: %SYS-SP-2-INTSCHED: 'idle' at level 2 -Process= "Port-Security" |
| CSCsx98446 | — | power consumption of act/stb sup720 has inconsistent behavior |
| CSCsy01275 | — | W15::  SYS-2-MALLOCFAIL: Memory allocation message seen after bootup |
| CSCsy01763 | — | 15 - 20 packets leek to DST with PACL after SSO |
| CSCsy03133 | — | TestNonDisruptiveLoopback skipped when run as scheduled test |
| CSCsy03141 | — | Copy of CSCsx06578 - to address the original hang problem in Mago |
| CSCsy08048 | — | CF Buffer Pools need to be scaled by platform |
| CSCsy08838 | — | Zamboni allows clear packet inbound on protected interface |
| CSCsy12800 | — | priv-lvl=15 should NOT be required for Local Web-Auth |
| CSCsy16220 | — | a switch may crash due to deadlock between snmp and eem |
| CSCsy20589 | — | Port diagnostic failures following 'redundancy reload shelf' command |
| CSCsy21797 | — | Cat6k-Unexpected SNMP messages occurred |
| CSCsy22802 | — | MPLS VPN broken, vrf connection  (permit missing for internal vlan acl) |
| CSCsy24522 | — | Cannot disable " errdisable detect cause dhcp-rate-limit "  12.2(33)SXI |
| CSCsy24691 | — | entPhysicalTable has power-input 3 Sensor for 6kW DC PS1 and not PS2 |
| CSCsy24895 | — | Memory leak in ACE HAPI process |
| CSCsy26526 | — | Router is getting crashed at netconf_sessionQs_set_max_message |
| CSCsy31098 | — | reconfigure pim snooping when configure static mrouter port |
| CSCsy32202 | — | 6500 IPSEC SPA SSO 'no crypto connect' cmd  causes stdby SUP reload |
| CSCsy34231 | — | EZVPN+VRF:Router reloads while unconfigure crypto map with traffic |
| CSCsy34566 | — | Disable VLAN mapping on ME6524, 6148A-GE-TX |
| CSCsy37175 | — | 2FE-PA Subintf lost connection after chassis/Flexwan2 reload |

| Identifier | Technology | Description |
|---|---|---|
| CSCsy37390 | — | Need to enable earl interrupt after earl initialization is done |
| CSCsy37652 | — | ws-ipsec-3 VSPA crashed in post frag processing |
| CSCsy38611 | — | Mcast traffic blackhole on uplink recvs after reload of RP switch |
| CSCsy41119 | — | C2W2B: Tracebacks observed on RP Console while MIP auto & service config |
| CSCsy41526 | — | PIM msgs duplicated when MPLS configured and IGMP Snooping Off on xface |
| CSCsy42216 | — | VSL Uptime Counter Reset and other Inaccuracies |
| CSCsy47281 | — | vlan distribution is not working in mago |
| CSCsy48986 | — | VSS: reload shelf shouldn't reload remote service module |
| CSCsy52376 | — | Sup crashes after numerous module resets |
| CSCsy53060 | — | 0315 ion image tcp.proc crash during bootup caused switch reloaded |
| CSCsy53336 | — | JQL:VSS:VSLcontrol link failure causes VSS unstability and won't recover |
| CSCsy54365 | — | frequent datapath recovery and traffic loss on WS-X6704 with DFC |
| CSCsy54583 | — | TTY data process on DFC leaks memory at prot_tty_malloc_named |
| CSCsy56389 | — | SLCP process is impacted by inserting/extracting modules |
| CSCsy56433 | — | Sh rom intermittently fails to display correct region info for standby |
| CSCsy58553 | — | Linecard reset causes traffic onto frr protected tunnel to be dropped |
| CSCsy61956 | — | Crash in ios-base when running 'show ip route' or 'show bgp' commands |
| CSCsy62160 | — | Vlan state unable to recover after shutdown by mac-limit |
| CSCsy62753 | — | MST configured router crashed after receiving PVST BPDU. |
| CSCsy66446 | — | %BIT-SP-4-OUTOFRANGE ltl_fpoe_defer_notify_with_pri on port-channel flap |
| CSCsy66794 | — | Module  Failed SCP dnld observed on ALL WAN CARDS with ISSU. |
| CSCsy69228 | — | Add CLI mls cef tunnel fragment support for non supertycho2 |
| CSCsy69740 | — | SXH: Traffic drop on L2 PO after cleared psecurity on rcving L2 ports |
| CSCsy75971 | — | %CWAN_HA-STBY-4-IFCFG_DFLT_LIST_ERROR messages seen on standby |
| CSCsy76728 | — | PfR: Egress BW measured for prefix is incorrect. |
| CSCsy78851 | — | Continous message:C6K_MPLS_LC-SP-3-INVALID_TE_IF_NUMBER  with atm bundle |
| CSCsy78994 | — | Memory leak in Service Task |
| CSCsy81934 | — | Non-standard static multicast MAC addresses lose ports after reload |
| CSCsy82121 | — | IGMP Source only not working due to MC_CAP not set |
| CSCsy83830 | — | IOS-RLB crashes while deleting the username sticky |
| CSCsy85171 | — | CDL2 Read Error: Time out |
| CSCsy86050 | — | MAC Move Notifications on VSS between active and down ports |
| CSCsy86252 | — | SP Crash printing "supervisor jamming EOBC.  It will be disabled." |
| CSCsy87619 | — | VSS port channel going down when powering down active switch |
| CSCsy90705 | — | GOLD intrusive test after earl reset causes network disruption |
| CSCsy94866 | — | C2W2B: CSM Config sync causes memory leak |
| CSCsy95520 | — | ~500msec Pkt loss after transition to HSRP Active on L3 int |

| Identifier | Technology | Description |
|---|---|---|
| CSCsy96102 | — | FM-4-MPLS_RSVD_VLAN_ERROR-failed to remove feature when vrf delete |
| CSCsz01254 | — | BIT-SW1_SP-4-OUTOFRANGE Message reported on VSS |
| CSCsz06187 | — | VACL capture for ingress software switched packets |
| CSCsz09329 | — | invalid display for show module command firmware version t_whit21@1.0 |
| CSCsz12369 | — | FPD support for SPA-8X1FE-TX-V2 is not enabled |
| CSCsz19246 | — | Crash after 'no dot1x port-control auto' |
| CSCsz22954 | — | Supported  WS-X6324-100FX-MM is powered down improperly |
| CSCsz23448 | — | SIP 200 not coming up and Router Crashes after applying card type E3 1 1 |
| CSCsz24554 | — | Statndby keeps rebooting. |
| CSCsz36826 | — | 6509E fan-tray failed to restore back to HP mode after OIR |
| CSCsz38798 | — | On SSO, Sup engine/DFC module get reset when MET set deleted |
| CSCsz40969 | — | Need to add Me_Kr flow-control status registers back into sierra/whitney |
| CSCsz44520 | — | trunk port in UDLD err-disable when native vlan is shutdown |
| CSCsz44678 | — | Tunnel won't forward traffic across global to vrf |
| CSCsz48086 | — | Default violate-action is missing from 3 color policy |
| CSCsz52069 | — | 2nd commit DDTS for CSCsz09329 |
| CSCsz53809 | — | Configuring vlan name containing space doesnt work across reload. |
| CSCsz55834 | — | GLBP may provided BIA MAC instead of Virtual MAC for mobile users |
| CSCsz56229 | — | Crashing after receiving an IGMP v2 Leave Message. |
| CSCsz62046 | — | Crash at memcpy after CPUHOG in SNMP ENGINE |
| CSCsz63359 | — | c2w2b:"show mls qos ip" displays vslot interface instead switchid and sl |
| CSCsz63721 | — | high cpu utilization when with 1000 policy and 1000 forced target |
| CSCsz67334 | — | ciscoEnvMonTemperatureStatus trap sent sporadically as NotFunctioning |
| CSCsz71904 | — | VSS switch crashed on pm_assert_fail |
| CSCsz71970 | — | c2w2b: Freed Memory being Accessed by lldp_med_free_local_annex |
| CSCsz74362 | — | Router crash @ af_policer_error_check |
| CSCsz74896 | — | VSS redundancy reload shelf X causes UDLD err-disable |
| CSCsz75820 | — | JQL: VSS hang on SP after RP crashed by software-forced reload |
| CSCsz83701 | — | W2B: SFP-UTP entPhysicalVendorType cevSFP1000BaseSx to zeroDotZero |
| CSCsz86787 | — | IPV6 mcast and IPV4 EMVPN VRF Lite traffic are not forwarded after SSO |
| CSCsz92137 | — | Crash in crypto_destroy_sadb_root() upon unconfiguring tunnel protection |
| CSCsz96469 | — | Tracebacks seen @chunk_free_with_pc while unconfiguring |
| CSCta06689 | — | Rapid PVST:mac address table not flushed after topology change |
| CSCta10870 | — | FPOE takes long time to be programmed on active vss switch |
| CSCta15415 | — | DHCP Snooping functionality is not working fine with private vlan |
| CSCta22749 | — | C2W2b: %CONST_DIAG-SW1_SP-3-BOOTUP_TEST_FAIL:LC powercyled during Multip |
| CSCta24027 | — | See c6k_power_port_mgmt.c:pd_get_sb 98 tracebacks at bootup |

| Identifier | Technology | Description |
|---|---|---|
| CSCta32922 | — | SP crash due to heartbeat failure. |
| CSCta57705 | — | C2W2b: reg_invoke_vs_ltl_src_index_changed() needs to be added on stdby. |
| CSCsr27727 | Content | Cat6K experiences a reload after %SYS-2-ASSERTION_FAILED: message |
| CSCsz36400 | Content | WCCP router may become confused with incompatible web-cache config |
| CSCej05426 | Infrastructure | HA AutoSAA issuing no rtr react 100001 forces stby into RPR mode |
| CSCse25551 | Infrastructure | IP SLA Group Schedule association with Individual Probes Forgotten . |
| CSCsj24186 | Infrastructure | %SYS-2-NOBLOCK messages from Pool Manager process |
| CSCsm66896 | Infrastructure | IP SLA Monitor strDupOctet memory leak |
| CSCso74665 | Infrastructure | C7600: Active SUP crashes when attaching to crashed FW |
| CSCsq73498 | Infrastructure | Dovetail: ciscoipc Crash Followed by RPC Timeout with MultiOS IPC |
| CSCsq74185 | Infrastructure | Image verification not possible on 12.2(33)SRC for the c7200 |
| CSCsr02336 | Infrastructure | long prompt delay after delete harddisk:core/* |
| CSCsr08750 | Infrastructure | router is crashing after giving the command memory reserve critical 1 |
| CSCsr94474 | Infrastructure | Running-config stuck: nv_csb_semaphore locked during copy run ftp |
| CSCsu53150 | Infrastructure | Tracebacks on ISSU RV  xdr_mcast_notify_event |
| CSCsv54929 | Infrastructure | Cannot save banner bigger than 2048 characters |
| CSCsv90106 | Infrastructure | nested crash leads to incomplete crashinfo |
| CSCsw14433 | Infrastructure | at UBR10K ISSU RV, ipc_do_delayed_init() sometimes delay 1 sec |
| CSCsw61555 | Infrastructure | Router Crashes after doing SSO |
| CSCsw96293 | Infrastructure | Reload in SNMP Proxy Forwarder after IOS upgrade |
| CSCsx42732 | Infrastructure | IOS64: IP-SLA configuration fails due to memory alloc failure on stby |
| CSCsx55240 | Infrastructure | Router crashes at html_config_command |
| CSCsy24676 | Infrastructure | IFS returns false success on error conditions |
| CSCsy45455 | Infrastructure | get-next request of rttMonJitterStatsEntry table fails |
| CSCsy55455 | Infrastructure | Crash at saaComponentGet |
| CSCsy61259 | Infrastructure | IFS buff cache goes into infinite loop on driver errors |
| CSCsy78382 | Infrastructure | sending non IP traffic causes IOSD crash |
| CSCsy86078 | Infrastructure | Memory corruption Failure |
| CSCsz19466 | Infrastructure | C2W1: int range command with port-channel load-defer cause router crash |
| CSCsz21732 | Infrastructure | Reload in SNMP at snmpProxyFwderSearchReq |
| CSCsz52815 | Infrastructure | Crash when 'history hours-of-statistics-kept' has value greater than 9 |
| CSCed01880 | IPServices | Not able to configure NAT tcp timeouts beyond 4194 sec |
| CSCef58137 | IPServices | Router Crash after high CPU, when IPNAT configured with route-map |
| CSCsa41736 | IPServices | Router crash after enable NAT rate-limit feature |
| CSCse66643 | IPServices | SYS-2-NOBLOCK error when redistributing NAT routes |
| CSCsg31017 | IPServices | parser view (role based cli) not applied when access via RSH |
| CSCsh49973 | IPServices | NAT-ALG corrupts offset value of DNS PTR response |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj76907 | IPServices | IPv6 UDP sockets may incorrectly show "--any--" for local address |
| CSCsm42110 | IPServices | IGMPv3 - Multicast router ignores IGMP leave when SSM mapping configured |
| CSCso50205 | IPServices | DNS based SSM mapping creates interface throttles when DNS is not avail |
| CSCsr69932 | IPServices | Stale HSRP packets are being processed instead of discarded |
| CSCsw51864 | IPServices | CHUNKFREE error and crash when changing NAT config |
| CSCsw52416 | IPServices | NAT: dynamic nat entries do not timeout in certain case |
| CSCsx23602 | IPServices | crash after 'clear ip nat trans *' |
| CSCsx33622 | IPServices | Fix MSS calcuation issue in TCP |
| CSCsx34372 | IPServices | c2w21/C2W2b:OSPF is not working with udlr/ude |
| CSCsx58889 | IPServices | Call fails under load intermittently with cause 47 no resource avail |
| CSCsx63640 | IPServices | Device gets crash @ tcp_find_conn_info |
| CSCsx74657 | IPServices | Many issues with NAT/Multicast feature |
| CSCsy26750 | IPServices | 6k Crash with ipnat_ldap_fixup (Redundancy Checks needed) |
| CSCsy39623 | IPServices | cannot ping local vlan interface ip address with NAT configured |
| CSCsy39667 | IPServices | dhcp-proxy-client incorrectly sends DHCPRELEASE in PPP-agg use-case |
| CSCsy45371 | IPServices | NAT: two static nat entry related issues |
| CSCsy74796 | IPServices | Memory leak at ip_multicast_ctl (when creating/deleting interfaces?) |
| CSCsy76195 | IPServices | standby delay timer does not take correct effect if set to >254 seconds |
| CSCsy77298 | IPServices | [DHCPD] IOS DHCP server does not send back option 82 in DHCPNAK |
| CSCsy97506 | IPServices | All nat'ed multicast packets punted to software |
| CSCsz12488 | IPServices | LDAP add with malformed BER attributes causes CPUHOG and MALLOCFAIL |
| CSCsz16580 | IPServices | [UNI]Active RP's CPU% spikes by MLD process after reload or longevity |
| CSCsz89107 | IPServices | high cpu due to ip_input process during SNMP trap |
| CSCsx61048 | LegacyProtocols | %SYS-3-TIMERNEG: negative offset -Process= "IPX RIP In" |
| CSCsz71787 | LegacyProtocols | Router crash by crafted IP packet. |
| CSCsw66153 | Management | Native vlan not displayed in show cdp neighbor detail |
| CSCsx30903 | Management | parser issues in global config mode |
| CSCsx46383 | Management | No SNMP response on Cat6K for IP-FORWARD-MIB with VRF and SNMP Contexts |
| CSCsy17342 | Management | router reload on removing cns config notify interval |
| CSCsx74883 | MPLS | c2w2b: Standby crash @ vrf_delete_if_ready while unconfiguring vrf inte |
| CSCsy29604 | MPLS | VRF leaking on the same router cause CEF to break |
| CSCsy60668 | MPLS | W1.5:: Toggle "mpls tra router-id" cause router crash |
| CSCsz11877 | MPLS | MPLS-TE Tunnel label re-allocation on mid-point router while RSVP-GR |
| CSCsz75180 | MPLS | Crash due to mpls subintf being removed |
| CSCsz92368 | MPLS | MDEBUG-2-ACCESSFREED: @tc_handle_dead_peers Enabling/disabling "mpls ip" |
| CSCsx15396 | Multicast | Mcast IIF stays up while physical interface is down |
| CSCsx28948 | Multicast | I/O Memory leak on 7200 |

| Identifier | Technology | Description |
|---|---|---|
| CSCsx34506 | Multicast | RPF failure with no PIM neighbor triggers PIM Hello |
| CSCsx53084 | Multicast | Multiple groups fail with autorp |
| CSCsx58861 | Multicast | Crash due to Stack for iGMP process running low |
| CSCsy72207 | Multicast | multicast rate-limit not applied to new (*,G) entries |
| CSCsy80910 | Multicast | Invalid ICMPv6 packet is sent after transmitting MLD reports |
| CSCsy96184 | Multicast | PIM should not reject assert with all zero source if RPT bit is set |
| CSCsz48668 | Multicast | SYS-2-BADSHARE: Bad refcount in datagram_done |
| CSCsk04590 | PPP | tx cpu crash at blt_pak_holdq_peek on shutdown of a member link |
| CSCsm93088 | PPP | MPPP toward DOM Nortel Active but not traffic crossing |
| CSCsw20267 | PPP | MLP APS across SPA does show in the routing table after failover |
| CSCee63182 | QoS | Router crashes while implementing rate-limit |
| CSCek42590 | QoS | alignment error seen at rsvp_first_object_type & rsvp_next_object |
| CSCsm97014 | QoS | Connectivity breaks for QOS + header compression on virtual templates |
| CSCsv91699 | QoS | "Transmitted pkts/bytes" column showing 0 packets on LSS SIP400 |
| CSCsy26097 | QoS | Traceback seen applying Unsupported HFQ Policy |
| CSCsy28998 | QoS | Spurious memory access and tracebacks On Boot |
| CSCeh66610 | Routing | Min hold time from neighbor is not seen in the configuration |
| CSCsk96581 | Routing | BGP sessions fail to establish after int flap due to hold timer expired |
| CSCsq11897 | Routing | Spurious memory seen at idb_get_ip_addrs and idb_get_ip_unnum |
| CSCsq20928 | Routing | CEFv6 dropping IPv6 unicast packets |
| CSCsq58289 | Routing | redistributed connected prefixes not seen as LSA 5 in ospf database. |
| CSCsr05431 | Routing | After SSO, cef removed vrf routes before bgp graceful timers time-out |
| CSCsr09208 | Routing | Memory allocation error of  fragmentation when plenty memory available. |
| CSCsr50704 | Routing | dmzlink-bw programs wrong traffic share count in routing table |
| CSCsr51801 | Routing | upon router reload some of the route-maps not permitting the prefixes. |
| CSCsr72352 | Routing | 6peinterascrr:Incorrect nexthop advertised between the routereflectors |
| CSCsr84530 | Routing | Static route not properly redistributed into BGP -- backout CSCsl92283 |
| CSCsu11161 | Routing | Neighbor x.x.x.x default-originate issues seen in 12.2 code |
| CSCsu61953 | Routing | Labels not getting allocated for BGP prefixes |
| CSCsu92300 | Routing | "sh ip mroute" shows some routes in pruned state |
| CSCsu96698 | Routing | BGP: /32 route being advertised while 'summary-only' is configured |
| CSCsv73754 | Routing | crash during vrf unconfig - bgp_vpn_impq_add_vrfs_cfg_changes |
| CSCsv91628 | Routing | BGP prefixes not exchanged between Route refectors through MP-EBGP |
| CSCsw29664 | Routing | running and startup config out of sync after iprouting.iosproc restart |
| CSCsw72680 | Routing | IP - Packets loop if running Microsoft NLB in presence of PIM |
| CSCsw73196 | Routing | bgp session flap btw GSR and 7600 due to illegal net(MDT grp addr issue) |
| CSCsw99768 | Routing | BGP malformed update sent |

| Identifier | Technology | Description |
|---|---|---|
| CSCsx03301 | Routing | Router crashed @ bgp_reset_rcache |
| CSCsx06457 | Routing | BGP may modify routes it does not own |
| CSCsx08294 | Routing | OSPF encounters a bus error crash when running SPF |
| CSCsx18270 | Routing | EIGRP: tags from version 2 peers are not displayed in topology table |
| CSCsx20177 | Routing | "no int loopback" causes stuck prefix in isis level-2 database |
| CSCsx21482 | Routing | Router crashes at ipv6_rip_nvgen_interface when issue wr mem command |
| CSCsx35205 | Routing | Standby ip arp entry is not reinstalled after static arp entry removed |
| CSCsx39310 | Routing | VRRP sends ARP req with Physical MAC if using same virtual IP as int IP |
| CSCsx47651 | Routing | IP LSRR broken with ip unnumbered |
| CSCsx51299 | Routing | Crash when remove and configure ipv6 ACL via telnet and console |
| CSCsx75004 | Routing | BGP CSC-PE advertises wrong out-label. |
| CSCsx96069 | Routing | OSPFv3 maxage LSA remains after Area-ID change |
| CSCsx98673 | Routing | PE not send extended-community to a peer newly added to peer-group |
| CSCsx99015 | Routing | crash if OSPF redistributes another OSPF and interface bw changes |
| CSCsy15150 | Routing | 33SXH5: Traceback @ isis_router when default interface configured |
| CSCsy27394 | Routing | Lawful Intercept Tap visible via show ip interface (sub-interface) |
| CSCsy27511 | Routing | 4basn: Issue generating update for pfx w/ 255 as# to old speaker |
| CSCsy28394 | Routing | Tracebacks when attaching 62000 loopback interfaces to OSPF |
| CSCsy29534 | Routing | Bus error crash on removing address-familly in router rip config mode |
| CSCsy32000 | Routing | Rtr crash on rcv routes w LinkLocal NH from v6 direct-connected IBGP nbr |
| CSCsy45838 | Routing | show ip ospf border-router crashing router |
| CSCsy58115 | Routing | Continuous BGP mem increase with non established neighbors |
| CSCsy73123 | Routing | Connected route on port-channel subintf not removed when Po is down |
| CSCsy76404 | Routing | Modular IOS: memory leak in CEF background process |
| CSCsy77842 | Routing | TB isis_process_no_router after isis router process deleted |
| CSCsy84134 | Routing | ARP table is flushed when deleting secondary IP address |
| CSCsy96019 | Routing | router reload @ ippkt_check with debug ip packet turned on |
| CSCsz16724 | Routing | BGPv6: default-metric is not being NVGEN'ed and not functionting |
| CSCsz42043 | Routing | OSPF originating orphan TE LSA |
| CSCsz55293 | Routing | wrongly marking IPv4 capability as negotiated, with peer only IPv6 sessi |
| CSCsz61156 | Routing | NH is not stored in BGP table when IPv6 VRF is redistributed |
| CSCsz78992 | Routing | Packet drops when "ip cef accounting per-prefix" configured |
| CSCsd91182 | Security | crypto pki export pkcs12 hangs when used with SCP |
| CSCsv20285 | Security | Whitney:Authentication to the CA server failed using ION. |
| CSCsv23797 | Security | SSH:Crash seen on 7200 on mcp_dev |
| CSCsv46973 | Security | "Change Password" is not properly relyaed |
| CSCsw50991 | Security | Traceback if underlying interface of 6to4 tunnel goes down. |

| Identifier | Technology | Description |
|---|---|---|
| CSCsy16177 | Security | scp:copy to router over sshv2 fails with  invalid checksum error |
| CSCsy17893 | Security | Ping to itself doesn't work on IPIP tunnels |
| CSCsy22311 | Security | SCP b/w IOS routers fails while the client is receiving file from server |
| CSCsz40612 | Security | GRE keepalive retry behavior is wrong |
| CSCsi05069 | WAN | DCE Sub-interface is not coming up after provisioning |
| CSCsw31019 | WAN | Router crashes while configuring the command "frame-relay be 1" |

## Caveats Resolved in Release 12.2(33)SXI1

### Resolved AAA Caveats

- CSCsv06973—Resolved in 12.2(33)SXI1

  **Symptom:**

  Router crashes For Authentication RESPONSE with GETUSER and when getuser-header-flags is modified and sent.

  **Conditions:**

  TACACS single-connection is configured. When authorization is configured Telnet to router and removing authorization,telnet to router again

  **Workaround:**

  Do not use TACACS single-connection option.

- CSCsv38166—Resolved in 12.2(33)SXI1

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp.

- CSCef52919—Resolved in 12.2(33)SXI1

  **Symptoms:** A privilege level 1 user is able to log in with a higher privilege level.

**Conditions:** This symptom is observed on a Cisco platform when the **aaa new-model** command is enabled, when the **privilege level** *level* command is present under the vty lines, and when the *level* argument has any value from 2 through 15.

**Workaround:** Do not configure privilege level 1 but configure any other privilege level.

- CSCsv73509—Resolved in 12.2(33)SXI1

  **Symptoms:** When "no aaa new-model" is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

  **Conditions:** Configure "no aaa new-model", configure **login local** under **line vty 0 4** and configure **login tacacs** under **line vty 0 4**.

  **Workaround:** There is no workaround.

#### Resolved IPServices Caveats

- CSCsr29468—Resolved in 12.2(33)SXI1

  Cisco IOS Software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- CSCsv04836—Resolved in 12.2(33)SXI1

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24.

- CSCsw18636—Resolved in 12.2(33)SXI1

  **Symptoms:** High CPU utilization occurs after device receives a ARP packet with protocol type as 0x1000.

  **Conditions:** This problem occurs on Supervisor 32 running Cisco IOS Release 12.2(33)SXI. This problem may also occur on Supervisor 720. The problem is only seen when you have bridge-group CLI being used, which leads to ARP packets with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

  **Workaround:** Filter the ARP packet. The device configuration should have bridge-group creation first, followed by interface-specific bridge-group options.

### Resolved LAN Caveats

- CSCsv05934—Resolved in 12.2(33)SXI1

  **Summary:** Cisco's VTP protocol implementation in some versions of Cisco IOS and CatOS may be vulnerable to a DoS attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash (and reload/hang). The crafted packet must be received on a switch interface configured to operate as a trunk port.

  **Workarounds:** There are no workarounds available for this vulnerability.

  This response is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20081105-vtp

### Resolved Multicast Caveats

- CSCso90058—Resolved in 12.2(33)SXI1

  **Symptoms:** MSFC crashes with Red Zone memory corruption.

  **Conditions:** This problem is seen when processing an Auto-RP packet and NAT is enabled.

  **Workaround:** There is no workaround.

- CSCsu79754—Resolved in 12.2(33)SXI1

  **Symptoms:** PIM packets may be processed on interfaces which PIM is not explicitly configured.

  **Conditions:** Unknown at this time.

  **Workarounds:** Create an ACL to drop PIM packets to such interfaces.

### Resolved Routing Caveats

- CSCsx10140—Resolved in 12.2(33)SXI1

  Recent research (1) has shown that it is possible to cause BGP sessions to remotely reset by injecting invalid data, specifically AS_CONFED_SEQUENCE data, into the AS4_PATH attribute provided to store 4-byte ASN paths. Since AS4_PATH is an optional transitive attribute, the invalid data will be transited through many intermediate ASes which will not examine the content. For this bug to be triggered, an operator does not have to be actively using 4-byte AS support.

  The root cause of this problem is the Cisco implementation of RFC 4893 (4-byte ASN support) - this RFC states that AS_CONFED_SEQUENCE data in the AS4_PATH attribute is invalid. However, it does not explicitely state what to do if such invalid data is received, so the Cisco implemention of this RFC sends a BGP NOTIFICATION message to the peer and the BGP session is terminated.

  RFC 4893 is in the process of getting updated to avoid this problem, and the fix for this bug implements the proposed change. The proposed change is as follows:

  "To prevent the possible propagation of confederation path segments outside of a confederation, the path segment types AS_CONFED_SEQUENCE and AS_CONFED_SET [RFC5065] are declared invalid for the AS4_PATH attribute. A NEW BGP speaker MUST NOT send these path segment types in the AS4_PATH attribute of an UPDATE message. A NEW BGP speaker that receives these path segment types in the AS4_PATH attribute of an UPDATE message MUST discard these path segments, adjust the relevant attribute fields accordingly, and continue processing the UPDATE message."

  The only affected version of Cisco IOS that supports RFC 4893 is 12.0(32)S12, released in December 2008.

  (1) For more information please visit:

http://www.merit.edu/mail.archives/nanog/msg14345.html

- CSCsx73770—Resolved in 12.2(33)SXI1

  **Symptom:** A Cisco IOS device that receives a BGP update message and as a result of AS prepending needs to send an update downstream that would have over 255 AS hops will send an invalid formatted update. This update when received by a downstream BGP speaker triggers a NOTIFICATION back to the sender which results in the BGP session being reset.

  **Conditions:** This problem is seen when a Cisco IOS device receives a BGP update and due to a combination of either inbound, outbound, or both AS prepending it needs to send an update downstream that has more than 255 AS hops.

  **Workaround:** The workaround is to implement **bgp maxas-limit X** on the device that after prepending would need to send an update with over 255 AS hops. Since IOS limits the route-map prepending value to 10 the most that could be added is 21 AS hops (10 on ingress, 10 on egress, and 1 for normal eBGP AS hop addition). Therefore, a conservative value to configure would be 200 to prevent this condition.

#### Other Resolved Caveats in Release 12.2(33)SXI1

| Identifier | Technology | Description |
|---|---|---|
| CSCeg80842 | — | PA-MC-8TE1 controller stuck ( similar to CSCdz72292 ) |
| CSCek70131 | — | SIP1 crash at vip_mlp_fastsend with HEARTBEAT error for mlppp qos |
| CSCek71010 | — | TB seen at bgp_oer_notify_pep bgp_oer_remove_path bgp_bestpath_old |
| CSCek77516 | — | PPC:SUP720:4k:SW-EoMPLS:%SW_MGR-SP-3-CM_ERROR_CLASS: Connection Mana |
| CSCse82480 | — | ip vrf receive cmd adds connected routes to VRF even interface down |
| CSCsf08092 | — | Deprecate tracking 'rtr' cmd in favour of 'ip sla' cmd |
| CSCsg83756 | — | SPA-8XCHT1/E1 after Reload C/A LED green even if no cable plugged |
| CSCsg87290 | — | SIP1-ChOC3: Extra path flap is observed on ChOC3 SPA interfaces |
| CSCsh22225 | — | CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR: |
| CSCsh54232 | — | Remove external loop option for nx1GE SPAs |
| CSCsi66012 | — | 2 garbage values in show module csm x ft details |
| CSCsi78584 | — | T3/E3 SPA:Line protocol is not comin up with E3 and framing bypass |
| CSCsj19308 | — | PE and CE ping fails over multilink ppp bundle. . |
| CSCsj80015 | — | Enhance logic for accurately detecting Semaphore Hog |
| CSCsk30196 | — | BADBUFFER error at pak_copy_contiguous_to_contiguous |
| CSCsk98751 | — | Router crash after issue command "mpls tra backup-path tunnel" |
| CSCsl44170 | — | LI tapped PPPoE LCP/PPP control packets originated from router are bogus |
| CSCsl46159 | — | Cost Minimization Feature keeps moving the traffic and doesn't stabilize |
| CSCsl99156 | — | No_Global bit out of syn between IPRM and BGP, when label no change |
| CSCsm01389 | — | Crash after clearing Auto-tunnel backup |
| CSCsm44147 | — | SSO failure due to mismatched command on SRB1 |
| CSCsm72121 | — | W2: bad cookie magic was detected after SSO switchover with sh vtp count |
| CSCsm74948 | — | mVPN RP does not send join to directed connected neigbor PE |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm75818 | — | Wrong OIL for data-mdt mroutes: multicast traffic loss |
| CSCsm76792 | — | PM HA bulk sync posting RF_DONE before bulk sync has finished |
| CSCsm83256 | — | IDSM2 Data port operation status not OK after boot OR SSO |
| CSCsm96309 | — | OIR-SP-4-WARN message displayed when PS1 or FAN removed |
| CSCso29141 | — | DFC installs drop index for MAC-address |
| CSCso35659 | — | L3 traffic rate limited after adding and removing Xcon to a SVI |
| CSCso36570 | — | es20 layer 2 interfaces can be configured with MTU other than jumbomtu |
| CSCso48665 | — | vlan filter can't be removed totally |
| CSCso51749 | — | GRE: policing functionality not working with multicast traffic |
| CSCso59242 | — | sierra: show mem detailed all stat is truncated. |
| CSCso59974 | — | BGP session goes idle after SSO switchover |
| CSCso88183 | — | DOME:dumper.proc crashes on dome when another process crashes |
| CSCsq07729 | — | VSS: flowcontrol incompatible msg when standby switch port add in bundle |
| CSCsq25028 | — | Malloc errors with IPC buffers on a Flex-wan |
| CSCsq31605 | — | auth_mgr:session stuck in Running state if clear auth issued during auth |
| CSCsq48025 | — | DACL is not getting programmed untill next Probe interval. |
| CSCsq56941 | — | 6500 - Static MAC cleared from port-channel member ints after reload |
| CSCsq73122 | — | Proxy-ARP returns BIA instead of VMAC with LAM |
| CSCsq82865 | — | Parsing error reading route-map match statements if longer than 254 chrs |
| CSCsq87496 | — | "%OIR-6-INSCARD" syslog not being send from the device |
| CSCsq96144 | — | Netflow v9 Exported Data issue in case of ECMP |
| CSCsr04190 | — | Traceback and standby SUP4 reloads after multiple standby resets |
| CSCsr09062 | — | MLP+QoS - Memory corruption with WRED configured |
| CSCsr15812 | — | Traceback: %SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error: on Congo |
| CSCsr22282 | — | All the trap entries are cleared on any port flap in the same vlan |
| CSCsr27980 | — | %C10K_QOS_GENERAL-3-EREVENT: Error @ ../toaster/c10k_rp/mce_qos.c:mce_qo |
| CSCsr29559 | — | WCCP flap corrupts mcast CEF adjacency |
| CSCsr37131 | — | buginf calls in l2trace when 'debug l2trace' is disabled |
| CSCsr44036 | — | IVFS is not supported, using internal matrix table msgs on router bootup |
| CSCsr56465 | — | With diag Off seeing %CONST_DIAG-SP-3-HM_TEST_FAIL on x6708 LC |
| CSCsr63098 | — | VRF-Aware Smart-Call Home requirement |
| CSCsr63831 | — | show platform hardware capacity fabric - incorrect % and time-SXH3 |
| CSCsr64777 | — | EPA crash, Corrupted redzone blk, netflow v5 |
| CSCsr68212 | — | MVRF name may get truncated if the VRF name is long |
| CSCsr88845 | — | unicast BootP replies dropped by DHCP snooping |
| CSCsu01372 | — | 33SB: Result of boot config command not sync to standby RP after reload |
| CSCsu04446 | — | PfR MC/BR crashes under stress with test traffic |

| Identifier | Technology | Description |
|---|---|---|
| CSCsu05721 | — | C2W2: %NTI-SP-3-AGENT_ERR and TB was seen after issu runversion |
| CSCsu07931 | — | cbQosPoliceConformedByte64 counter displays aggregate instead conformed |
| CSCsu10022 | — | L2 traffic is policed when CoPP is enabled |
| CSCsu10261 | — | BFD ISSU peer reload between mcp_dev and sierra image |
| CSCsu25699 | — | OER ICMP Probes using incorrect outbound interface when encrypted |
| CSCsu36715 | — | W2.0 : C2 : ION : Memory Leak in MSDP process |
| CSCsu36836 | — | Conflict when using sockets and files at the same time |
| CSCsu44534 | — | Sup NSF/SSO causes 4 sec traffic loss over EC with uplink ports. |
| CSCsu45210 | — | Upgrade 12.2SXF-> 12.2SXH with Port-Security causes standby boot loop |
| CSCsu45786 | — | Crash on show tcp br after tcp process restart |
| CSCsu46124 | — | SVI ifInMulticastPkts ifOutMulticastPkts are always zero |
| CSCsu49257 | — | Cstn-id timer should be restarted when access-request is seen |
| CSCsu50611 | — | PfR Master Controller crash when shut/no shut |
| CSCsu67559 | — | Copy Run Start does not provide the same functionality as 'wr mem' |
| CSCsu69660 | — | ldcache crashed due to Process Deadlock b/w installer and ldcache proc |
| CSCsu72026 | — | OER MC reports max report limit reach when request all exit links report |
| CSCsu72496 | — | %PM-3-INTERNALERROR: Port Manager Internal Software Error |
| CSCsu75546 | — | C2W21: traffic not span to NAM using span conf mode local-tx source intf |
| CSCsu77945 | — | PfR echo probe shows 0 completes |
| CSCsu81158 | — | Pkt drops on SIP-400 LC due to QoS lock fail for subintfs. |
| CSCsu81838 | — | SA : memory leak @ slb_gtp_echo_response |
| CSCsu82580 | — | 6VPE : Traffic dropped under stress configuration with more then 3Kvlan |
| CSCsu83563 | — | MMLS:If rate-lt on when STDBY reloads, doesnt work on swovr:x40/dual RSP |
| CSCsu84927 | — | c2w2:allow DIVC to negotiate red mode when matrix overide check is yes |
| CSCsu85166 | — | Crash @ hwidb_get_firstsw after SSO. |
| CSCsu86524 | — | IKMP process leak: check_ipsec_proposal |
| CSCsu88008 | — | c2w2:standby HSRP router crashed @mcast_igmp_process_join |
| CSCsu88471 | — | Err "Insertion of mld_s_g_type in the grp WAVL tree failed" after SSO |
| CSCsu88557 | — | [no] mdix auto" CLI command not present for WS-X6196-RJ21" |
| CSCsu90369 | — | Whitney2: %XDR-DFC4-6-ISSUBADRCVTFM_DUMP Traceback on Switchover |
| CSCsu91714 | — | IGMP-JOIN is lost from SUP to MSFC |
| CSCsu92395 | — | Crash caused by event manager configuration: "action mail" |
| CSCsu93936 | — | PM_SCP-SP-2-LCP_FW_ERR_INFORM for WS-X6548-GETX-45AF |
| CSCsu95237 | — | SSO switchover,clear packet seen on the wire exposing the inner IP pkt |
| CSCsu95605 | — | Route-map with "match route-type local" not functioning properly |
| CSCsu95662 | — | W2: VSL config got error in mixed type with interface range cmd |
| CSCsu97020 | — | policer on flexwan/multilink is dropping even CIR is not reached |

| Identifier | Technology | Description |
|---|---|---|
| CSCsu97418 | — | Standby PRE is resetting when doing "write mem" |
| CSCsv01136 | — | Traffic don't get forwarded after iprouting restart then do SSO with PBR |
| CSCsv04471 | — | CDP 2nd port notification traceback |
| CSCsv07313 | — | SPA timeout observed on reload with scalable access-lists config. |
| CSCsv07858 | — | IfIndex for unconfigured VLAN on 7613 |
| CSCsv09249 | — | VSS after dual-active recovery MEC on standby chassis UDLD error disable |
| CSCsv17989 | — | interface in SIP200 show "admin down" when it is physical down |
| CSCsv18681 | — | CLI "sh int transceiver properties switch 1" also display switch 2 ports |
| CSCsv20339 | — | MN history table is flooded with multiple (~500) add/delete entries |
| CSCsv20920 | — | telnet from a GRE tunnel to real address for DNS vserver fails |
| CSCsv21612 | — | High CPU on SP due to PM Callback process with VTP pruning enabled |
| CSCsv21770 | — | PAC re-provisioning fails, AAA generates endless number of Prov Requests |
| CSCsv22779 | — | VRF-PBR: Packets dropped with reflexive acl |
| CSCsv22913 | — | igmp snooping querier disabled when static mrouter port is configured |
| CSCsv24742 | — | PfR exit link is OOP when interface counter wraps |
| CSCsv28564 | — | Policy Base Forwarding marks the packets to cos5 on VSS |
| CSCsv30307 | — | ISSU is broken because of CSCsg52337 commit in SRC |
| CSCsv30679 | — | Sup detetes Vlans from Sup IDSM Config on startup / failover |
| CSCsv32101 | — | QoS: memory corruption traceback when using access-list with time range |
| CSCsv34159 | — | Access control based on EAP, not on Radius type, in conflicting messages |
| CSCsv36306 | — | BFD: Removing BGP on the router makes the neigh router crash |
| CSCsv36698 | — | IPC Open Port Errors observed on 7600-SSC-400/VPN-SPA |
| CSCsv36892 | — | New CLI goto tclsh if previous CLI with tclsh terminated abnormally |
| CSCsv37543 | — | GRE/IPsec misconfig is only resovled through module or chassis reload |
| CSCsv38928 | — | IGMP Snooping does not send out Global query on  2nd  TCN < 35 seconds |
| CSCsv39228 | — | VSS-The system didn't display SN of SFP correctly |
| CSCsv39496 | — | TB@rfsc_issu_negotiate_and_open_server_port on RPR upgarde from W1 to W2 |
| CSCsv40523 | — | WISM: Gig interfaces show as unknown(4) |
| CSCsv40770 | — | %ICC_ISSU_NEGO-SP-3-OPEN_PORT_RELIABLE: Can't open reliable port |
| CSCsv40974 | — | "wism mod <mod> controller <1 |
| CSCsv43991 | — | FWSM's internal portchannel on the cat6k side goes down after upgrading |
| CSCsv44923 | — | MAC move behind phone leads to lost connectivity with MAB |
| CSCsv52426 | — | GRE Recirc index is 0x0 in adjacency hence encap operation fails on DFC |
| CSCsv52941 | — | EEM24: snmp-notif ed policies not triggered after removal and add |
| CSCsv53392 | — | "Mls qos trust device cisco-phone" causes instabilty on the system |
| CSCsv56974 | — | OIR WAN Module w/VPN/SPA interfaces. does not take down Vlan/Tunnels |
| CSCsv57235 | — | duplex is changing automatically on WS-X6148-RJ-45 |

| Identifier | Technology | Description |
|---|---|---|
| CSCsv57305 | — | VSS: software forced reload with 100Mbps SFPs in supervisor uplink ports |
| CSCsv58013 | — | MLPPP policy-map could not be deleted. |
| CSCsv58279 | — | Reload due to Address Error with multicast configuration |
| CSCsv60643 | — | sup4 when toggled 10g mode the config is not synced to standby sup |
| CSCsv63799 | — | PfR MC/BR bus error crash in ip fast flow |
| CSCsv64079 | — | SXF7: Patching fails with WiSM Card on Cat6500 |
| CSCsv66513 | — | PBR controlled application not in DEFAULT with exit interface  shutdown. |
| CSCsv66706 | — | IDSM port-channel Allowed-Vlan statements lost on reload |
| CSCsv66827 | — | Clearing the SSH session from a different vty session crashes the box. |
| CSCsv73299 | — | L2 multicast forwarding broken with DHCP snooping & TTL rate-limiter |
| CSCsv73721 | — | ISSU ERP tracebacks on active RP during router bootup |
| CSCsv76509 | — | Cat6k/MSTP in compat mode BPDUs sent in VLAN1 regardless of config |
| CSCsv80075 | — | Pre-release Feature Card VS-F6K-PFC3C (227) |
| CSCsv86288 | — | Sending a hello response with a session-id element causes a crash |
| CSCsv91278 | — | MPLS interface wedged following upgrade to SXI |
| CSCsv92872 | — | 10GE link on Sup720-10GE takes more than 30sec to go down during crash |
| CSCsw17478 | — | PVT HOSTS- ports programmed with incorrect rdt index upon bootup |
| CSCsw18793 | — | VRF-PBR: TCAM adjacency not programmed with multiset policy order after |
| CSCsw32280 | — | Diag error on WS-X6148A-45AF card asic with Traffic |
| CSCsw41168 | — | %ALIGN-3-SPURIOUS at sm_get_portEntPhyIndex |
| CSCsw41439 | — | W21,VSL,SNMP,cvsCoreSwitchPreempt,cvsCoreSwitchPriority not SSO aware. |
| CSCsw41706 | — | router reload when registering EEM service diag script |
| CSCsw43953 | — | Card not identified SIP Is OIR'd during Standby SUP bootup |
| CSCsw45396 | — | when STP recovered in uplinkfast,no sent dummy multicast packets |
| CSCsw48181 | — | Unknown Unicast is dropped on Shut/no Shut of a VLAN |
| CSCsw48824 | — | Switchport Block Unicast - prevents RTP on same VLAN |
| CSCsw51395 | — | Proper handling is required for Mac-Filter with Port-security |
| CSCsw52819 | — | Kernel dumper needs a few enhancements. |
| CSCsw53362 | — | c2w2b: Device crashes with NAT stress test |
| CSCsw73302 | — | memory leak in qm_increment_ag_policer_usage on standby-rp |
| CSCsw75589 | — | ip flow-cache mpls label-positions can lead to bus error under load |
| CSCsw78806 | — | Router getting crashed at lat_int_command |
| CSCsw82732 | — | VPN-SPA internal vlan interface wedged in SXH4 |
| CSCsw87352 | — | 6748's port can not forwarding traffic - port src index wrong |
| CSCsw87399 | — | auth_mgr: crash @ eap_show_context when doing show eap session |
| CSCsw87563 | — | packets with multicast mac and unicast ip are software routed by cat6500 |
| CSCsw90798 | — | Bus error crash after configuring vlan name change |

| Identifier | Technology | Description |
|---|---|---|
| CSCsw93969 | — | %ICC_ISSU_NEGO-SP-3-OPEN_PORT_RELIABLE: Can't open reliable port |
| CSCsw98231 | — | SDBY stuck @ CEF RRP RF Client(5025) after ISSU RV |
| CSCsx06578 | — | SIERRA:MAGO switch got crashed after reload with SIERRA_INTEG_090106 |
| CSCsx09273 | — | WEBAUTH(IP adm) is not INITiating if IPDT entry already exists. |
| CSCsx10011 | — | VSS: IO memory leak from pre_process_vsibc_vsda_pak |
| CSCsx15038 | — | NVgen issue with violate-action commands under policy-map class |
| CSCsx15138 | — | Crash at qos_feature_get_fo |
| CSCsx16206 | — | Traffic loss issue from SFM capable modules to other device through DEC |
| CSCsx26114 | — | IOS tagging certain commands as level 1 in config mode |
| CSCsx28532 | — | VPN SPA freezes when ip mtu changed on tunnel interface |
| CSCsx29645 | — | IPv6 Multicast traffic can not converge after SSO |
| CSCsx32416 | — | BFD session flaps during router/LC bootup after reload |
| CSCsx34570 | — | VSS:remove port-channel from interface causes other members to go down |
| CSCsx37615 | — | VSS: rem comm standby-rp sh plat hardware capacity may reset switch |
| CSCsx48991 | — | Disable LI CLI |
| CSCsx49718 | — | Auth Man Single-host-Guest VLAN doesn't trigger reauth on EAPOL start |
| CSCsx53257 | — | Minor diag error - TestNetflowShortcut failed |
| CSCsx55543 | — | auth_mgr: with vlan assignment reauthentication takes 30sec to start |
| CSCsx58786 | — | Router crash @ routemap_track_nexthop |
| CSCsx62912 | — | W2: update the PM switch vp limits for MST, PVST and Rapid-PVST |
| CSCsx64668 | — | Config change on port of WS-X6148-FE-SFP will move other ports to down |
| CSCsx76308 | — | HA client crashing attempting to free unassigned memory |
| CSCsy03141 | — | Copy of CSCsx06578 - to address the original hang problem in Mago |
| CSCsc78999 | AAA | Address Error exception at TPLUS |
| CSCsk40765 | AAA | crash due to AAA/TACACS+ server-private re-configuration |
| CSCsq37815 | AAA | Case sensitive Username authentication is passed with wrong user name |
| CSCsq94524 | AAA | "aaa accounting update newinfo" causes extra "jitter maximum 0" option |
| CSCsr70963 | AAA | Crash when remove DEAD radius server from config |
| CSCsv02117 | AAA | session flapping cause %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs |
| CSCsw17553 | AAA | Radius-server pac keyword is not nvgened when used with automated tester |
| CSCsw19816 | AAA | cat6000: IOS login enhancments not creating logs for telnet with AAA |
| CSCek78237 | ATM | High CPU on ATM PA Helper process on PA-A3-T3 |
| CSCso64050 | ATM | HA functionality is not working when policy attached to atm pvc |
| CSCsr86103 | ATM | ATMoMPLS: Traffic stops flowing on applying service-policy on atm pvc |
| CSCsr27727 | Content | Cat6K experiences a reload after %SYS-2-ASSERTION_FAILED: message |
| CSCsx40747 | Content | Router hangs while doing ip casa configurations |
| CSCef82896 | Infrastructure | When removing the user name from auth dialog, http crashes |

| Identifier | Technology | Description |
|---|---|---|
| CSCin79116 | Infrastructure | show memory summary could push the CPU util to 100% |
| CSCsc77704 | Infrastructure | region_find_by_addr goes into infinite loop when spurious memory occurs. |
| CSCsc86307 | Infrastructure | c3845  crashed @ show_systat |
| CSCse41523 | Infrastructure | bootldr config caused stbyPRE reset if file does not exist on stby-bootf |
| CSCse49151 | Infrastructure | 3800 clock slip over times verified in lab |
| CSCsh85011 | Infrastructure | DSGS7: Router crash at saaEnhancedHistoryFreeTab |
| CSCsj46707 | Infrastructure | ubr7200 G1 hangs during bootup |
| CSCsj57479 | Infrastructure | Traceback found at data_inconsistency_error_with_original_ra |
| CSCsj87744 | Infrastructure | Parser mode change issues |
| CSCsk80396 | Infrastructure | Inconsistant router Crash seen when jitter operation takes place |
| CSCsl61281 | Infrastructure | Show logging command should be a privileged command |
| CSCsm33221 | Infrastructure | IP SLA Probe type DHCP with no relay-agent IP add. on Dhcp disc. packet |
| CSCsm54810 | Infrastructure | router stops producing the auth-proxy login page intermittently |
| CSCso21611 | Infrastructure | Crash at internal idb counter increment function |
| CSCsq73498 | Infrastructure | Dovetail: ciscoipc Crash Followed by RPC Timeout with MultiOS IPC |
| CSCsr07557 | Infrastructure | Memory leak in parser_chunk_malloc after get/set on Auth Framework obj |
| CSCsr50834 | Infrastructure | CPU HOG after changing logging buffered up to 50MB |
| CSCsr60789 | Infrastructure | W1.3: VSL crash after preemptive switchover in ifs_open_file_decrement |
| CSCsu57889 | Infrastructure | banner exec CLI ignoring lines starting with #, !, and ; |
| CSCsu78906 | Infrastructure | Wrong "%SYS-5-CONFIG_I: Configured from x.x.x.x by snmp" messages |
| CSCsv34988 | Infrastructure | Console/Telnet/SSH login banner not properly formated after upgrade |
| CSCsv50606 | Infrastructure | SNMP: ISSU incompatibility with message type 20 |
| CSCsv80900 | Infrastructure | W21:: EARL-SPSTBY-2-SWITCH_BUS_IDLE & PF_ASIC-SPSTBY-3-ASIC_DUMP @boot |
| CSCsv86766 | Infrastructure | Signature fail while copy, causing system:/running-config to be deleted |
| CSCsw15188 | Infrastructure | Router crashes with "debug isdn q931" enabled |
| CSCsw16658 | Infrastructure | Unavailable ipv6 ACL prevent configuring ipv4 ACL |
| CSCsw35917 | Infrastructure | SP syslog messages not sent as SNMP traps by RP's SNMP agent |
| CSCsw51126 | Infrastructure | High CPU on Virtual Exec process after vty session timeout exec setup |
| CSCsw61555 | Infrastructure | Router Crashes after doing SSO |
| CSCsw76894 | Infrastructure | Problems faced with ipv6 SNMP when ipv4 address is not configured |
| CSCsx32841 | Infrastructure | ceImageDescription may exceed 255 characters |
| CSCek10384 | IPServices | 7200 NAT dropping Out to In ESP Packets |
| CSCsl11712 | IPServices | Router crashes when DGVPN is configured with VRF . . |
| CSCsm89795 | IPServices | Orbitty repeatedly Crashes  - Succeptible to Denial of service attacks |
| CSCso39062 | IPServices | C2W2: %SYS-3-INVMEMINT: Invalid memory action message & TB's with PAT. |
| CSCso54027 | IPServices | Spurious memory access in ttcp_rcv_stats |
| CSCsq14311 | IPServices | 7200 crash - ipnat_unlock_parent_entry (PPTP) |

| Identifier | Technology | Description |
|---|---|---|
| CSCsq22397 | IPServices | DLSw peer connection initiated from interface IP and not local-peer IP |
| CSCsq81365 | IPServices | MFI: UDP forwarded-protocols from VRF are leaked into global table |
| CSCsu38774 | IPServices | FTP'ing a file from a router will fail if the FTP account cannot delete |
| CSCsu64215 | IPServices | ip tcp adjust-mss command results in packet loss for non-TCP traffic |
| CSCsu67461 | IPServices | Router crashes when "show track brief" entered |
| CSCsu72176 | IPServices | Crash:Process Deadlock  in Standby while reloading UUT with DHCP configs |
| CSCsu74400 | IPServices | File descriptor leak with FTP of a DHCP database |
| CSCsu77597 | IPServices | Frames with virtual MAC dest address are dropped with bridging enabled |
| CSCsu95319 | IPServices | IGMP report was not sent to helper address. |
| CSCsv12265 | IPServices | HSRP stuck in INIT when learning and if address changed |
| CSCsv16987 | IPServices | nat pool size more than 16 bit long should not be configured |
| CSCsv27480 | IPServices | VRRP MAC aging out due to being stored as dynamic entry after reload |
| CSCsv54324 | IPServices | HSRP stuck in INIT state after a reload on a c3845 gig-eth interface |
| CSCsv54510 | IPServices | Router is not getting pruned after shutting the interface |
| CSCsv56160 | IPServices | BGP session flap due to TCP selective-ack |
| CSCsv86201 | IPServices | Modular IOS : max sockets overflow |
| CSCsv99443 | IPServices | standby delay reload doesn't work on SUP/RSP720 |
| CSCsw16698 | IPServices | DHCP database could not be locked DHCPD process could not lock semaphore |
| CSCsw64000 | IPServices | 3800: Ethernet controller wrongly programmed when using DHCP and PIM |
| CSCsw66082 | IPServices | Router crash seen at ip_mcast_address_lookup in ssm-map router |
| CSCsw73391 | IPServices | ip igmp limit gets stuck |
| CSCsw96272 | IPServices | nat overload command not translating packets |
| CSCsx09343 | IPServices | Name resolution triggers pager in non-interactive mode. |
| CSCsx32283 | IPServices | Malformed L field in LDAP crashes 6k with NAT |
| CSCsr04069 | LAN | ifOutOctets for vlan subint with GTS/ratelimit is inaccurate |
| CSCsw81485 | LegacyProtocols | Unconfiguring IPX crashes the switch |
| CSCsb84797 | Management | ATM or FR main interface resets when disabling CDP or deleting subint |
| CSCse29570 | Management | router crashes when pulling config from CNS containing no config initial |
| CSCso35250 | Management | unexpected reload while communicating with CNS server |
| CSCsu10229 | Management | The cdpCacheAddress mib not providing GLOBAL_UNICAST Address |
| CSCsv48296 | Management | cns image retrieve  command is forcing to router crash |
| CSCsv93351 | Management | CNS ID Change unexpectedly |
| CSCsq49176 | MPLS | 7200 Bus error crash on invalid address, charlotte_post_coalesce_rx |
| CSCsr15969 | MPLS | MPLS TE: extended tunnel id may not be 0.0.0.0 |
| CSCsu50374 | MPLS | FRR tunnels doesn't go down if TE flooding is disabled on the headend. |
| CSCsv00773 | MPLS | Loose Path Reopt not applied when link costs changed |
| CSCsv13738 | MPLS | slow convergence when use vrf definition instead of ip vrf |

| Identifier | Technology | Description |
|---|---|---|
| CSCsv31126 | MPLS | snmpwalk of mplsTunnelTable may not show all MPLS TE Tunnels |
| CSCsv41456 | MPLS | Tracebacks seen at IFMGR-3-DUP_IFINDEXifDescr"Virtual-Access2-mpls layer |
| CSCsv62004 | MPLS | standby crashes with ipbase image and VRF config |
| CSCsw35638 | MPLS | FRR Interoperability issue between Juniper PLR and IOS MP |
| CSCsw82028 | MPLS | BGP graceful restart is not supported on IP service image |
| CSCsb77148 | Multicast | sh ip mpacket x.x.x.x quality output is wrong after counter wraps around |
| CSCsc52732 | Multicast | Enabling PIM on sub-IF causes mcast packet drops on other sub-IF |
| CSCsl32142 | Multicast | crash from memory corruption from malformed auto-rp Multicast |
| CSCsl52213 | Multicast | PIM assert timer mechanism problem |
| CSCsu86494 | Multicast | Assert flag is not cleared after PIM neighbor loss |
| CSCsv29659 | Multicast | RP configured inside the nat not shown on uut outside the nat |
| CSCsw29463 | Multicast | The adjacency/oce lookup should not be done in mcast fast switching path |
| CSCsw36940 | Multicast | Router crashed at "mrm_manager_sender_commands" |
| CSCsx15396 | Multicast | Mcast IIF stays up while physical interface is down |
| CSCsf07760 | PPP | MLP:  Crashes/buffer leaks when large number of sessions come up at once |
| CSCsr81271 | PPP | Invalid VCD error messages upon PVC flap |
| CSCsu70011 | PPP | ipv6 static route pointing to multilink (flexwan) dissapears after sso |
| CSCsh39945 | QoS | PRE3:Router crash with 'show int random' with 40k+ pppoeovlan sessions |
| CSCsh57935 | QoS | %RSVP-3-BAD_RSVP_MSG_RCVD_AUTH_WIN after shut/no shut |
| CSCsl94263 | QoS | Router crash at stile_update_fast_flag due to random-detect dscp-base |
| CSCsm28515 | QoS | Marking not happening on FlexWAN interface with SXH  after oir/reload |
| CSCso97991 | QoS | policy with bc value less than default(4ms) will cause drops on WAN int |
| CSCsq55678 | QoS | c2w2: Policy on control-plane is not working with acl log option |
| CSCsr05501 | QoS | % NBAR Error: hwidb could not found shows up when reload |
| CSCsv12372 | QoS | Spurious memory access @ fr_oqueue |
| CSCsv85791 | QoS | Flexwan+/PA-MC-2T3+ introduce 5+ seconds delay on egress |
| CSCsv91699 | QoS | "Transmitted pkts/bytes" column showing 0 packets on LSS SIP400 |
| CSCsw36285 | QoS | Incorrect Police rate  under calss-default |
| CSCee30355 | Routing | Memory leak at ip_multicast_ctl |
| CSCef65457 | Routing | EIGRP and RIP advertise null0 static routes after they are removed |
| CSCef67010 | Routing | NHRP registrations shouldn't do a routing table lookup |
| CSCsb15164 | Routing | Security holes while configuring a standard ACE with host address |
| CSCsc98813 | Routing | Set metric in route-map effects other RIP routes hop count |
| CSCsd25753 | Routing | BGP Aggregated supernet routes not Advertised properly |
| CSCse45978 | Routing | BGP to RIP redistribution breaks as RIP nexthop moves to alternate path |
| CSCse68877 | Routing | CEF/BGP table MPLS label mismatch YW3 Non Multi-path |
| CSCsh54161 | Routing | dune, Nov image goes unstable - creates eigrp routing loops |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj42399 | Routing | Redistributed static covered by network statement sets metric to 0 |
| CSCsk87526 | Routing | T/B  ipv6_rib_process_changeQ after shut cmd applied  Int. running RIPng |
| CSCsm63632 | Routing | Continuous XDR IPC errors (inability to create an IPC buffer)/Watermark |
| CSCso56038 | Routing | %DUAL-3-INTERNAL traceback at igrp2_packet_community_add_item |
| CSCso90107 | Routing | SNMP: bgpPeertable and cbgpPeertable shows only results for ipv4 peers |
| CSCsq36206 | Routing | MDT tunnels not getting created on 7206 Device |
| CSCsr01403 | Routing | cefswitching2.1:More time taken(12 mts) to converge after Adjacency flap |
| CSCsr21670 | Routing | elected more routes than expected routes as multipath |
| CSCsr40997 | Routing | IPv6 RIP: Unconfiguring RIP from an interface doesn't update RIB on peer |
| CSCsr67361 | Routing | I/O memory leaks when BGP neighbor points to a local address |
| CSCsr88705 | Routing | BGP route getting lost after "shut/no shut" of BGP peering interface |
| CSCsu01272 | Routing | MPLS PE 7600 changes RT when a BGP soft clear is executed |
| CSCsu05464 | Routing | System out of mem on SSO switchover with more than 32K ipv6 ref-acl flow |
| CSCsu06447 | Routing | EIGRP:static route redistribution not working with distribution-list |
| CSCsu08935 | Routing | bgp as-override on 2 byte PE does not overwrite AS 23456 properly |
| CSCsu32217 | Routing | Redistribution from BGP to OSPF vrf fails for high metric prefixes |
| CSCsu39689 | Routing | crash @ipv6_nd_prefix_delete_by_handle with rip 6pe_scaling_performance |
| CSCsu42077 | Routing | next entries didnot function after added new entry on ACL |
| CSCsu53624 | Routing | bgp multicast shows unicast information in show ipv6 protocol |
| CSCsu62356 | Routing | RIPNG 'last gasp' message not seen on Interface down in some IOS branch |
| CSCsu63996 | Routing | OSPF flaps after SSO switchover causes traffic loss after SSO switchover |
| CSCsu69767 | Routing | Global to VRF and VPN import route-map depends on configuration order |
| CSCsu76993 | Routing | EIGRP:Routes not tagged with match source redistribution-source |
| CSCsu79988 | Routing | 4BASN: BGP path/bestpath memory usage is 14% higher |
| CSCsu86338 | Routing | <cr> missing in ip extcommunity-list command |
| CSCsu97177 | Routing | switch crashes querying (old) IPv6 MIB |
| CSCsu97834 | Routing | On module reset, 'ip route' statement loses 'name' argument |
| CSCsv00604 | Routing | IPv6 host with static default route still learns ND default router |
| CSCsv01474 | Routing | 'ip rip advertise' command  lost after interface flap/clear ip route |
| CSCsv05009 | Routing | %OSPF-4-FLOOD_WAR: error during heavy flaps for type-5 and type-7 LSAs |
| CSCsv17933 | Routing | Static route in VRF is not redistributed by RIP after link flap |
| CSCsv27607 | Routing | BGP: Outbound route-map updating withdraw only one member |
| CSCsv51298 | Routing | c3825 faces chunk memory leak @ bgp_do_ipv4redist_callback |
| CSCsv59334 | Routing | Connected nets redistr from eigrpTObgp when  no net 0 is set under eigrp |
| CSCsv62777 | Routing | High CPU process caused by stucked VTY line |
| CSCsv85052 | Routing | Crash observed when "ispf" is issued in vty with ip routing disabled |
| CSCsv89643 | Routing | OSPF: MAC address of next hop unresolved on ptp eth by adjacency bringup |

| Identifier | Technology | Description |
|---|---|---|
| CSCsv97472 | Routing | CSCso62166_dcq_issue_rn_walktree_timed_locking is changed |
| CSCsw24286 | Routing | TE tunnel bandwidth command breaks isis topology |
| CSCsw24611 | Routing | Router crashes at bgp_set_path_attr |
| CSCsw24826 | Routing | OSPF crash during type-9 maxage |
| CSCsw30941 | Routing | ospfNbrStateChange trap sent by non-DR |
| CSCsw65441 | Routing | ARP packets drops due to excessive ARP requests sourced from SVI |
| CSCsw65933 | Routing | Prefix not learned from PE to CE |
| CSCsw79397 | Routing | Device crashing at bgp_command_af_specific |
| CSCsw89080 | Routing | changed L1 area address not updated in L2 lsp with multi-area config |
| CSCsw92379 | Routing | Crash seen on releasing snooping bindings after LC OIR |
| CSCsx11776 | Routing | show ip bgp version 1 causes router crash |
| CSCsx15841 | Routing | aggregate-address does not NVGEN upon switchover on cat6k |
| CSCsx17446 | Routing | Tunnel route and a non-tunnel (IGP) route with same metric (TE metric) |
| CSCsx18270 | Routing | EIGRP: tags from version 2 peers are not displayed in topology table |
| CSCea11368 | Security | CRL fetch using ldap fails if vrf configured in trustpoint |
| CSCeg49153 | Security | PKI: crl checking takes too long to timeout if the server is down |
| CSCeh75136 | Security | TACACS+ rem_addr field empty after first SSH authen attempt fails |
| CSCsc91824 | Security | SSH from router disconnects vty session if there is no matching cipher |
| CSCse80892 | Security | isakmp-profiles and VRFs: IPSEC sa fails to come up for the below config |
| CSCsk22496 | Security | Router crashes @ssh_command when remoove crypto key |
| CSCsm70719 | Security | Memory allocated @ add_new_cdp_to_list Leaked |
| CSCsq51052 | Security | SSH server on IOS reporting bogus protocol version |
| CSCsu54801 | Security | Cannot get s/w adjacency header information on DFC for IPv6 in v6 tunnel |
| CSCsu90280 | Security | NHRP IPv6 registration not working |
| CSCsv86113 | Security | On modular IOS, SSH on VRF int is allowed irrespective of vrf-also key |
| CSCsv04674 | VPDN | Random Vector AVP in ICCN isn't marked as Mandatory |
| CSCsv04733 | VPDN | A LAC might diconnect a tunnel by StopCCN for tunnel-passwords > 31 char |
| CSCsv68584 | VPDN | LAC crashed @sw_mgr_cm_inQ_handler/free |
| CSCsw78939 | VPDN | PDSN(LAC) fails to bring up the VPDN calls after stressing for long time |
| CSCso62193 | WAN | Standby resets due to parser return error "no frame-relay vc-bundle" |
| CSCsq47900 | WAN | OIR operation on POS interfaces with APS result in ALIGN error |

## Caveats Resolved in Release 12.2(33)SXI

### Resolved AAA Caveats

- CSCsa43465—Resolved in 12.2(33)SXI

  **Symptoms:** Users may be able to access root view mode (privilege level) 15 without entering a password.

  **Conditions:** This symptom is observed on a Cisco router that has the Role-Based CLI Access feature enabled and occurs when the **none** keyword is enabled in the default login method list.

  For example, the symptom may occur when you enter the **aaa authentication login default group tacacs+ none**. When the TACACS+ server is down, users are allowed to enter non-privileged mode. However, users can also access the root view through the **enable view** command without having to enter a password.

  **Workaround:** Ensure that the **none** keyword is not part of the default login method list.

  Further Problem Description: The fix for this caveat places the authentication of the **enable view** command in the default login method list.

### Resolved Infrastructure Caveats

- CSCse85652—Resolved in 12.2(33)SXI

  **Symptom:** The Cisco IOS HTTP server and the Cisco IOS HTTPS server provide web server functionality to be used by other Cisco IOS features that require it to function. For example, embedded device managers available for some Cisco IOS devices need the Cisco IOS HTTP server or the Cisco IOS HTTPS server to be enabled as a prerequisite.

  One of the functionalities provided by the Cisco IOS HTTP server and the Cisco IOS HTTPS server is the WEB_EXEC module, which is the HTTP-based IOS EXEC Server. The WEB_EXEC module allows for both “show” and “configure” commands to be executed on the device through requests sent over the HTTP protocol.

  Both the Cisco IOS HTTP server and the Cisco IOS HTTPS server use the locally configured enable password (configured by using the **enable password** or **enable secret** commands) as the default authentication mechanism for any request received. Other mechanisms can also be configured to authenticate requests to the HTTP or HTTPS interface. Some of those mechanisms are the local user database, an external RADIUS server or an external TACACS+ server.

  If an enable password is not present in the device configuration, and no other mechanism has been configured to authenticate requests to the HTTP interface, the Cisco IOS HTTP server and the Cisco IOS HTTPS server may execute any command received without requiring authentication. Any commands up to and including commands that require privilege level 15 might then be executed on the device. Privilege level 15 is the highest privilege level on Cisco IOS devices.

  **Conditions:** For a Cisco IOS device to be affected by this issue all of the following conditions must be met:

  - An enable password is not present in the device configuration
  - Either the Cisco IOS HTTP server or the Cisco IOS HTTPS server is enabled
  - No other authentication mechanism has been configured for access to the Cisco IOS HTTP server or Cisco IOS HTTPS server. Such mechanisms might include the local user database, RADIUS (Remote Authentication Dial In User Service), or TACACS+ (Terminal Access Controller Access-Control System)

The Cisco IOS HTTP server is enabled by default on some Cisco IOS releases.

**Workaround:** Any of the following workarounds can be implemented:

- Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an enable password

  Customers requiring the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server must configure an authentication mechanism for any requests received. One option is to use the **enable password** or **enable secret** commands to configure an enable password. The enable password is the default authentication mechanism used by both the Cisco IOS HTTP server and the Cisco IOS HTTPS server if no other method has been configured.

  In order to configure an enable password by using the **enable secret** command, add the following line to the device configuration:

  ```
  enable secret mypassword
  ```

  Replace *mypassword* with a strong password of your choosing. For guidance on selecting strong passwords, please refer to your site security policy. The document entitled "Cisco IOS Password Encryption Facts" explains the differences between using the **enable secret** and the **enable password** commands to configure an enable password. This document is available at the following link:
  http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml

- Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an authentication mechanism other than the default

  Configure an authentication mechanism for access to the Cisco IOS HTTP server or the Cisco IOS HTTPS server other than the default. Such authentication mechanism can be the local user database, an external RADIUS server, an external TACACS+ server or a previously defined AAA (Authentication, Authorization and Accounting) method. As the procedure to enable an authentication mechanism for the Cisco IOS HTTP server and the Cisco IOS HTTPS server varies across Cisco IOS releases and considering other additional factors, no example will be provided. Customers looking for information about how to configure an authentication mechanism for the Cisco IOS HTTP server and for the Cisco IOS HTTPS server are encouraged to read the document entitled "AAA Control of the IOS HTTP Server", which is available at the following link:
  http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml

- Disabling the Cisco IOS HTTP Server and/or the Cisco IOS HTTPS server functionality

  Customers who do not require the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server can disable it by adding the following commands to the device configuration:

  ```
  no ip http server no ip http secure-server
  ```

  The second command might return an error message if the Cisco IOS version installed and running on the device does not support the HTTPS server feature. This error message is harmless and can safely be ignored.

  Please be aware that disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server may impact other features that rely on it. As an example, disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server will disable access to any embedded device manager installed on the device.

**Further Problem Description:** In addition to the explicit workarounds detailed above it is highly recommended that customers limit access to Cisco IOS HTTP server and the Cisco IOS HTTPS server to only trusted management hosts. Information on how to restrict access to the Cisco IOS HTTP server and the Cisco IOS HTTPS server based on IP addresses is available at the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/https/configuration/12-4/nm-http-web.html#GUID-BB57C0D5-71DB-47C5-9C11-8146773D1127

Customers are also advised to review the "Management Plane" section of the document entitled "Cisco Guide to Harden Cisco IOS Devices" for additional recommendations to secure management connections to Cisco IOS devices. This document is available at the following link: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

- CSCsr72301—Resolved in 12.2(33)SXI

  **Symptom:** Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http

  **Conditions:** See "Additional Information" section in the posted response for further details.

  **Workarounds:** See "Workaround" section in the posted response for further details.

#### Resolved IPServices Caveats

- CSCsk64158—Resolved in 12.2(33)SXI

  Several features within Cisco IOS Software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory.

  This advisory is posted at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

- CSCsm45390—Resolved in 12.2(33)SXI

  **Symptom:** An IOS software crash may occur when receiving a specific malformed DHCP packet.

  **Conditions:** An IOS device configured for DHCP Server and receives a DHCP-request from a DHCP relay device. A specific malformed option in the packet packet may induce a software traceback or crash. The specific packet will not occur without manual modification.

  **Workaround:** None.

- CSCsm27071—Resolved in 12.2(33)SXI

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS Software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.

– The device may reload.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory.

The advisory is posted at
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- CSCek52673—Resolved in 12.2(33)SXI

  A router that has DHCP server enabled could reload after receiving a malformed UDP packet.

  **Workaround:** None

#### Resolved Routing Caveats

- CSCso64422—Resolved in 12.2(33)SXI

  **Symptom:** Cisco IOS router may crash after receiving malformed EIGRP packets.

  **Workaround:** Only allow EIGRP packet from trusted neighbours.

- CSCsm93548—Resolved in 12.2(33)SXI

  **Symptom:** Cisco IOS router may crash after receiving malformed EIGRP packets.

  **Workaround:** Only allow EIGRP packet from trusted neighbours.

#### Resolved Security Caveats

- CSCsi17158—Resolved in 12.2(33)SXI

  **Symptoms:** Devices running Cisco IOS may reload with the error message “System returned to ROM by abort at PC 0x0” when processing SSHv2 sessions. A switch crashes. We have a script running that will continuously ssh-v2 into the 3560 then close the session normally. If the vty line that is being used by SSHv2 sessions to the device is cleared while the SSH session is being processed, the next time an ssh into the device is done, the device will crash.

  **Conditions:** This problem is platform independent, but it has been seen on Cisco Catalyst 3560, Cisco Catalyst 3750 and Cisco Catalyst 4948 series switches. The issue is specific to SSH version 2, and its seen only when the box is under brute force attack. This crash is not seen under normal conditions.

  **Workaround:** There are mitigations to this vulnerability: For Cisco IOS, the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

  Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with ‘ssh’ removed from the list of permitted transports on VTY lines while in configuration mode. For example: **line vty 0 4 transport input telnet end**

  If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely using Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html

  More information on configuring ACLs can be found on the Cisco public website:
  http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

- CSCsj85065—Resolved in 12.2(33)SXI

  A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Cisco has released free software updates that address this vulnerability. Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl.

#### Resolved Unknown Caveats

- CSCsk93241—Resolved in 12.2(33)SXI

  Cisco IOS Software Multi Protocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi

- CSCsg35077—Resolved in 12.2(33)SXI

  **Symptoms:** A device that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message.

  **Conditions:** The device must have a valid and complete configuration for IPsec. IPsec VPN features in Cisco IOS software that use IKE include Site-to- Site VPN tunnels, EzVPN (server and remote), DMVPN, IPsec over GRE, and GET VPN.

  **Workaround:** Customers that do not require IPsec functionality on their devices can use the **no crypto isakmp enable** command in global configuration mode to disable the processing of IKE messages and eliminate device exposure.

  If IPsec is configured, this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.

  Further Problem Description: This bug is triggered deep into the IKE negotiation, and an exchange of messages between IKE peers is necessary.

  If IPsec is not configured, it is not possible to reach the point in the IKE negotiation where the bug exists.

#### Other Resolved Caveats in Release 12.2(33)SXI

| Identifier | Technology | Description |
|---|---|---|
| CSCdu79630 | AAA | Username on vty not displayed if accounting is not configured |
| CSCed69872 | AAA | TACACS+ directed request leaves hanging TCP session |
| CSCed93927 | AAA | %RADIUS-3-NOSERVERS: No Radius hosts configured although AAA is up |
| CSCee42617 | AAA | Remove/Re-enter global radius server command causes auth. failure |

| Identifier | Technology | Description |
|---|---|---|
| CSCee66606 | AAA | per-group deadtime is nvgend as 60x user input |
| CSCef27578 | AAA | The router crashes when test aaa stop CLI is issued |
| CSCef97900 | AAA | AAAA-3-DROPACCTLOWMEM warning message somewhat misleading |
| CSCeh84727 | AAA | LPIP ARP entries become incompleted after a while |
| CSCek32177 | AAA | TPLUS: Failed to decode AV addr=255.255.255.254 |
| CSCek77360 | AAA | Tacacs authentication failed for tcb_clear with pppoe |
| CSCir01788 | AAA | Unable to configure ip tacacs source-interface globally |
| CSCsc98046 | AAA | TACACS Accounting isn't sending stop time in the stop packet. |
| CSCsd48175 | AAA | AAA/TACACS not failing over to second server |
| CSCse02550 | AAA | ip radius source-interface not used in combination with vrf |
| CSCsg14301 | AAA | AAA/TACACS spurious memory accesses in tplus_handle_req_timeout |
| CSCsg18288 | AAA | Enable authentication ignores Tacacs+ configuration in rare situation |
| CSCsg48725 | AAA | TLB exception in tacacs_plus_get_conn |
| CSCsg82766 | AAA | Unexpected crash due to bus error in Cisco 3825 |
| CSCsh23142 | AAA | aaa local authentication not happening for authproxy . |
| CSCsh46990 | AAA | Console hangs with enable/line as aaa fall-back methods |
| CSCsh72214 | AAA | Login local denies valid authentication |
| CSCsi63598 | AAA | Bus error crash in tplus_server_key during TACACS+ configuration |
| CSCsi99473 | AAA | TACACS authorization fails with 'request for nonexistent server' msg . |
| CSCsj90016 | AAA | AAA ISSU Client support. |
| CSCsk06660 | AAA | Radius error in AAA blocking mode |
| CSCsl29214 | AAA | AAA server change leads to bus error crash after "show run" is issued |
| CSCsl47365 | AAA | TACACS+ authorization should ignore unknown attribute |
| CSCsl57645 | AAA | tacacs-server directed-request fails for enable authentication on 6500 |
| CSCsl97384 | AAA | Command 'show aaa user all' triggers IOS reload due to Bus Error |
| CSCsm84915 | AAA | Nas-port-type is missing in Access-request |
| CSCso25507 | AAA | Modem call with Tacacs failed @ Fail to set vrf socket option |
| CSCso95426 | AAA | Exposure of Radius-Keys in debugs. |
| CSCsq98160 | AAA | No communication between SW and AAA with IPBase image |
| CSCsr17680 | AAA | test aaa group server request failing over |
| CSCsr26098 | AAA | SSH/Telnet failed with IPBase image on Sup32 with AAA server |
| CSCsi91649 | Access | Input packets not cef switched |
| CSCsj88665 | Access | Bus error with PA-MC-2T3+ when deleting channel-group |
| CSCsl41784 | Access | ION: ARP Input memory leak with "mobile ip arp" |
| CSCeg52354 | ATM | Memory leak at pvcd_enqEvent |
| CSCei33231 | ATM | ATM PVC bundle protected group test failed with bumping exhausted |
| CSCek40952 | ATM | OIR of PA-A3-OC3MM= generates tracebacks on OIR |

| Identifier | Technology | Description |
|---|---|---|
| CSCek74474 | ATM | no/default proto ip inarp cmd ineffective until ATM VC bounced. |
| CSCsd84347 | ATM | PVC stops sending OAM loopback if AIS/RDI received |
| CSCse87275 | ATM | CEoP: shaping configuration does not work . |
| CSCsh34529 | ATM | autobahn76: ATM interface config lost on standby RP |
| CSCsh98378 | ATM | Router crashes at atm_create_vp_db |
| CSCsi72854 | ATM | Inconsistent IMA CLI after router reload . |
| CSCsj71998 | ATM | ATM interface lost its ipaddress after graceful stop/start of interface |
| CSCsj84931 | ATM | CEOP: after OIR with atm local switching and ima, router crashes |
| CSCsk01927 | ATM | oam-ac emulation, vc stays UP after shutting CE ATM interface down. |
| CSCsk72676 | ATM | Pvc not coming up after removing vc-class from it |
| CSCsu03608 | ATM | 7500 crash at loki_send_phy_config_ll when bringup IMA interface |
| CSCsj09149 | Content | WCCP: no redirection following change in configuration |
| CSCsl29993 | Content | WCCP Should Mark Client 'NOT Usable' with Missing L2 Adjacency |
| CSCsl65335 | Content | WCCP: reload following ACL update |
| CSCsm12247 | Content | WCCP: hash assignment may be lost after service group change |
| CSCsm32473 | Content | WCCP: system reload with path splitting and output redirection |
| CSCsm35350 | Content | WCCP GRE return breaks IPsec traffic AND/OR creates phantom packet count |
| CSCsm53427 | Content | WCCP: multicast + appliance shutdown leads to high CPU |
| CSCsq31981 | Content | WCCP: redirection does not work with CEF and ip accounting |
| CSCsq64362 | Content | running config for wccp has missing and duplicated services |
| CSCed33145 | Infrastructure | line vty exec-timeout not working properly, def causes spur mem acc |
| CSCeg16786 | Infrastructure | Device not loading with the image and SP crashes |
| CSCeg69540 | Infrastructure | 10k crash due to a bus error |
| CSCeh51638 | Infrastructure | Calling-Station-Id not send anymore for http admin |
| CSCeh54177 | Infrastructure | Mismatch of the index of ciscoMemoryPoolFree OID to its own value |
| CSCei86912 | Infrastructure | Router reloads unexpectedly while issuing GD commands |
| CSCek35108 | Infrastructure | Rommon truncates boot string to 64 characters |
| CSCek46087 | Infrastructure | IPC ack_pending not updated correctly |
| CSCek58956 | Infrastructure | Need process_ok_to_reschedule check in process_may_suspend |
| CSCek62770 | Infrastructure | bundles need to include CW_ strings |
| CSCek78644 | Infrastructure | SNMP replies do not source VRF interfacaes |
| CSCir01027 | Infrastructure | snmp over ipv6 is broken for cat6k_hi_fi |
| CSCsa53739 | Infrastructure | CISCO-CONFIG-COPY-MIB ccCopyProtocol does not work in 12.0(30)S on 7200 |
| CSCsa57468 | Infrastructure | rttmon-mib does not return getnext value when queried via snmp |
| CSCsa97971 | Infrastructure | IOS SLB TCP probe state toggles |
| CSCsb06920 | Infrastructure | SYS-3-MGDTIMER: Running timer -Process= SAA Event Processor |
| CSCsb98906 | Infrastructure | Memory Leak with bgp regexp deterministic configuration |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd23127 | Infrastructure | IPC-SP-2-LOCK IPC-SP-2-UNLOCK followed by tracebacks on SSO s/w |
| CSCsd37499 | Infrastructure | %IFS-3-FSMAX: Failed to add ?, maximum filesystems 64 msg with Traceback |
| CSCsd55059 | Infrastructure | polling CISCO-FLASH-MIB slows down GSR |
| CSCsd81275 | Infrastructure | Syncing the private configuration to the standby Router FAILED |
| CSCse07265 | Infrastructure | No syslog message generated for IP SLA timeout condition |
| CSCse40379 | Infrastructure | IP SLA: Increasing the request-data-size via CLI crashes the device. |
| CSCse40401 | Infrastructure | IP SLA Traceback: %SCHED-3-STUCKMTMR: Sleep with expired managed timer |
| CSCse66080 | Infrastructure | Memory leak from MallocLite @ physical_buffer_to_malloc() |
| CSCse72476 | Infrastructure | HTTP authen fails using Local followed by Radius Authorization for EXEC |
| CSCsg35587 | Infrastructure | Latest RTT for jitter calculated as RTT average with timeouts as zero |
| CSCsg82453 | Infrastructure | Syslog over TCP: should try to reconnect to the syslog server |
| CSCsg99677 | Infrastructure | Crashinfo files saved with wrong name CRASHI~1 |
| CSCsh40811 | Infrastructure | stbySP crashes with ActNotResp during FSU from SRA to SRB |
| CSCsh45091 | Infrastructure | Port fix for CSCed94684 for ws-c3750-24p |
| CSCsh47251 | Infrastructure | 3700 crashes as soon as loading image |
| CSCsh63508 | Infrastructure | disk0:/sys/cpmbit/base is busy, try again later msg on stby SP on SSO. |
| CSCsh66245 | Infrastructure | Lowest memory is too low after reload on Cisco 10000 |
| CSCsh81291 | Infrastructure | Exodus Mayflower C10K ISSU fails at loadversion |
| CSCsh85522 | Infrastructure | SNMP-Sever user CLI throwing trace back messages |
| CSCsh96179 | Infrastructure | IPSLA pathEcho probe doesn't complete for all hops |
| CSCsi22502 | Infrastructure | installer imf.tar file not being zipped creates uninstallable image |
| CSCsi43776 | Infrastructure | IPC: Invalid process name pointer; follow-up to CSCsh76558 . |
| CSCsi49008 | Infrastructure | SNMP sends responses to 0.0.0.0 when VRFs configured |
| CSCsi49890 | Infrastructure | SNMP: ciscoFlashFileEntry gives no index on disc with hidden files |
| CSCsi76486 | Infrastructure | ip http source-interface command ignores VRF |
| CSCsi88974 | Infrastructure | LI: Malloc failure on setting MD src interface as Loopback interface |
| CSCsj06593 | Infrastructure | CPU hog msgs for RFSS worker process and Async write process |
| CSCsj12867 | Infrastructure | Restart occurs after executing write memory command |
| CSCsj27963 | Infrastructure | Need graceful handling of full nvram |
| CSCsj52693 | Infrastructure | ospf neighbor flap with fast hellos and 16 neighbors |
| CSCsj52992 | Infrastructure | CPU hogs when configuring snmp-server host |
| CSCsj54596 | Infrastructure | logging userinfo command no longer accepted |
| CSCsj67434 | Infrastructure | The CLI: 'parser config cache interface' does not work |
| CSCsj80951 | Infrastructure | *Neutrino* proc reported memory Freed/Holding is incorrect |
| CSCsj83417 | Infrastructure | BOOM: addto_mempool_pc_array() message seen with show memory command |
| CSCsk03336 | Infrastructure | CEF process is unable to handle timer events when there are lot of Event |
| CSCsk06492 | Infrastructure | snmp-server drop vrf-traffic implementation in 12.2 SRB train |

| Identifier | Technology | Description |
|---|---|---|
| CSCsk09735 | Infrastructure | Router crashed on mkdir with 3dots,reload and show file system . |
| CSCsk10412 | Infrastructure | Config Sync: Bulk-sync failure due to BEM mismatch -parser view li-view |
| CSCsk13725 | Infrastructure | GSR: rttmon-mib does not return getnext value when queried via snmp |
| CSCsk27147 | Infrastructure | SNMP stops responding while polling from CISCO-MEMORYPOOL-MIB |
| CSCsk37278 | Infrastructure | BFD clients flaps when boot string is removed from "show running" . |
| CSCsk41686 | Infrastructure | PARSER-3-CFGLOG_NOMEM: constanlty in log |
| CSCsk42373 | Infrastructure | Memory leak in ctid_set_changetime function |
| CSCsk45467 | Infrastructure | Log overruns leaks buffers |
| CSCsk70446 | Infrastructure | NRT: tracebacks @ data_inconsistency_error - 7200 for HTTP config . |
| CSCsk71670 | Infrastructure | New active RP crashed at ipc_issu_process_timer_event() |
| CSCsk75147 | Infrastructure | CBS3120 LightSabre switch crashes during license install while reloading |
| CSCsk75310 | Infrastructure | UDP Echo: control message not sent out of correct interface. |
| CSCsk82972 | Infrastructure | copy running-config to startup-config does not work as expected |
| CSCsk91176 | Infrastructure | PXF crash causes IPC timeout to all linecards in the chassis |
| CSCsk99687 | Infrastructure | crash seen during ISSU runversion in ipc_open_port |
| CSCsl01595 | Infrastructure | c7600: Disable port-channel creation using 'interface range' command. |
| CSCsl16001 | Infrastructure | Booting from dosfs monlib is slow - needs performance improvement |
| CSCsl23306 | Infrastructure | RP crashes at ipc_check_flow_control with sso . |
| CSCsl33908 | Infrastructure | show ver truncates system's running image name  to 64 chars |
| CSCsl39860 | Infrastructure | Stdby Sup keeps rebooting w/SSO after running some SNMP CLI cmds |
| CSCsl52220 | Infrastructure | MF: "[no] snmp ifindex persist" enables persistence on other intf. |
| CSCsl53110 | Infrastructure | VSS: Stby rp crashes on boot |
| CSCsl58963 | Infrastructure | Manual OIR of pcmcia flash card crashes dosfs proc in Sup720 |
| CSCsl59629 | Infrastructure | Infinite Loop at ciscoFlashFileSize while doing snmpwalk |
| CSCsl60092 | Infrastructure | Active SP crashed @ipc_fragment_cleanup with VSL shut/no shut test |
| CSCsl64869 | Infrastructure | IP SLA: NumOfRTT & PacketLateArrival incremented for same packet |
| CSCsl70722 | Infrastructure | Router crash polling rttmon mib with active IP SLA probes |
| CSCsl97612 | Infrastructure | rttMonStats tables returns NULL values for snmpget |
| CSCsm01126 | Infrastructure | PRE-B crashes while in progress to standby cold-config |
| CSCsm01334 | Infrastructure | %failed to configure the mapping messages are seen on standby SUP. |
| CSCsm14366 | Infrastructure | Empty crash file generated on wan module crash at boot-up |
| CSCsm27493 | Infrastructure | procmib_server port has to send rpc reply only for RPC requests. |
| CSCsm32392 | Infrastructure | memory corruption  crash at nv_ifs_open and nv_ifs_close |
| CSCsm47417 | Infrastructure | W2:seting ceExtSysBootImageList cause "wr mem" not working correctly |
| CSCsm49218 | Infrastructure | Missing traceback for jump to zero exceptions |
| CSCsm77199 | Infrastructure | DATACORRUPTION-1-DATAINCONSISTENCY HTTP_FIND_FLASH_FILE |
| CSCsm89735 | Infrastructure | Router crashes on giving show idb after sessions are down in PPPOE-ipv6 |

| Identifier | Technology | Description |
|---|---|---|
| CSCso02960 | Infrastructure | %RTT-4-DuplicateEvent causes trackbacks after upgrading to 12.2(33)SXH |
| CSCso29361 | Infrastructure | cfg added under interface range vlan not being added in redundant sup |
| CSCso38185 | Infrastructure | IPSLA not handling invalid timestamp properly |
| CSCso48834 | Infrastructure | ip sla config with udp-jitter probe failed due to no connection |
| CSCso52837 | Infrastructure | Error while copying a file to disk0: |
| CSCso53866 | Infrastructure | Accepting interface range commands with or without whitespace is broken |
| CSCso57001 | Infrastructure | RP & SP crash after link flapping for CFM, IP SLA and EVC config |
| CSCso66862 | Infrastructure | ID Manager incorrectly returns ID contexts that are on the free list |
| CSCsq03621 | Infrastructure | Timestamps in "show rmon events" wrap at 2^32-1 milliseconds (7+ weeks) |
| CSCsq14340 | Infrastructure | Stale "snmp community-map" command  found in stand-by running config |
| CSCsq16325 | Infrastructure | Incomplete serial interface command creates interface |
| CSCsq19159 | Infrastructure | RP crashes in chassismib_add_sub_card_entry after linecard reload |
| CSCsq34676 | Infrastructure | Modular IOS: show process cpu sorted triggers unexpected reload |
| CSCsq35093 | Infrastructure | XDR-6-XDRIPCNOTIFY: Message not sent to slot 1/0 (1) because of IPC |
| CSCsq60922 | Infrastructure | Modular IOS:Router crashed with SNMP copy and with format in console |
| CSCsq64663 | Infrastructure | SUP32 crashed after deleting LACP etherchannel |
| CSCsr06282 | Infrastructure | DHCP operation and getmany on ciscoRttMonMIB crashes device |
| CSCsr09033 | Infrastructure | SNMP response contains source ip address as a broadcast ip address |
| CSCsr17757 | Infrastructure | IP SLA: Tail-drop with UDP-jitter test with num packets > 1000. |
| CSCsr18073 | Infrastructure | ipslaEtherJitterLatestSum2PosDS sum differs from show ipsla |
| CSCsr24171 | Infrastructure | snmpEngineTime not SSO aware, snmpFrameworkMIB |
| CSCsr31518 | Infrastructure | copy ftp://username:password failed to pass correct value. |
| CSCsr64361 | Infrastructure | Standby continously resetting due to SNMP RF client notification timeout |
| CSCsr68545 | Infrastructure | Error %DATACORRUPTION-1-DATAINCONSISTENCY when running ipsla with rtt |
| CSCsr84639 | Infrastructure | Standby-RP reload while syncing NOTOFICATION-LOG-MIB data |
| CSCsr97343 | Infrastructure | MSDP peer flaps randomly |
| CSCsu35597 | Infrastructure | Renaming a directory/file throws  error message |
| CSCsu37266 | Infrastructure | Modular IOS: tcp.proc terminated due to signal SIGSEGV |
| CSCsu39152 | Infrastructure | %IFMGR-4-NOIFINDEX adding interface Multilink [n] |
| CSCec51750 | IPServices | Router reloads do to bus error. and illegal access to low address |
| CSCec68752 | IPServices | crash due to CPUHOG and block overun on long nat route name string . |
| CSCec79570 | IPServices | UDP port 1985 opens |
| CSCeh69721 | IPServices | %SCHED-3-CORRUPT:Schedulerevent magic corrupted by TFTP Server |
| CSCek53084 | IPServices | ACL/ATOM client inject between REL4/REL3...2 |
| CSCek63433 | IPServices | rp crashed when multiple processes exits with shared sockets |
| CSCek65374 | IPServices | PRE3 startup-config parse failed on post sync4 exodus image |
| CSCek71379 | IPServices | %TCP-2-INVALIDTCB: Invalid TCB pointer:-Process= IP Input |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd66215 | IPServices | Arp reply not populating the bridge-table on 7200 router |
| CSCse01124 | IPServices | HSRP groups stuck in Init state if dampening cfgd on certain interfaces |
| CSCse87499 | IPServices | RF client timing out in PLATFORM_SYNC that lead to active reset |
| CSCsg21394 | IPServices | Router reload unexpectedly  by malformed DNS response packets |
| CSCsg49882 | IPServices | ip ftp source-interface ip address & interface chang after write mem |
| CSCsg60447 | IPServices | 7200: BVI stops receiving CLNS/ISIS packets |
| CSCsh15817 | IPServices | UDP socket events are not recevied by RTR responder process |
| CSCsi42225 | IPServices | We need improvement for ip igmp limit command |
| CSCsi42717 | IPServices | saa_vrf_test_udpe & saa_vrf_test_itter generate an unexpected error mess |
| CSCsi45840 | IPServices | ARP requests for HSRP virtual IP may fail after switchport cmd is used . |
| CSCsi66366 | IPServices | All transport protocols are displayed in running config for VTY |
| CSCsi66859 | IPServices | NSE-100: Router Crash when we send traffic with bridge-group config |
| CSCsi78892 | IPServices | Configuring bridge-group makes CPUHOG message. |
| CSCsi84742 | IPServices | DHCPv6 relay agent can't remove route when RELEASE lease time in nonzero |
| CSCsj29841 | IPServices | Port forwarding breaks NAT-overload on a 6509 |
| CSCsj41479 | IPServices | DHCP Services should not be enabled by default in IOS |
| CSCsj67110 | IPServices | HSRP: Stacklow message when unconfiguring interface |
| CSCsj83854 | IPServices | Incorrect static nat entries programmed in nat table |
| CSCsj93195 | IPServices | RP crashes at ipv4fib_les_switch_wrapper on configuring crypto map |
| CSCsk02920 | IPServices | TCP TSecr value invlalid - not zero and not last TSval from partner |
| CSCsk06539 | IPServices | bus error while unconfiguring static SSM mappings via TFTP . |
| CSCsk16821 | IPServices | DHCP does not NAK after DHCPREQUEST from unknown client . |
| CSCsk23972 | IPServices | Telnet failed with "No wild listener" error |
| CSCsk38763 | IPServices | Dhcp snooping  Ftp'ing of database is failing |
| CSCsk39022 | IPServices | Modular IOS: ip directed-broadcast not working |
| CSCsk39926 | IPServices | Unable to route local FTP traffic over VRF with IOS image |
| CSCsk47888 | IPServices | SRB2:standby keeps reloading due to Bulk-sync failure on PRC mismatch . |
| CSCsk68320 | IPServices | Reload on configuring "no ip routing" with MSDP configured |
| CSCsk81396 | IPServices | NAM process crash in 12.2SXF . |
| CSCsk83505 | IPServices | %L3_MGR-3-REQ_SEND:error packet allocation after Remote HL HW reset |
| CSCsk96976 | IPServices | DHCP Option 66 adds more quotation marks around URL after reload . |
| CSCsl06431 | IPServices | Modular IOS: Memory leak in udp.proc |
| CSCsl10348 | IPServices | Crash writing to or from ftp/tftp server in modular IOS |
| CSCsl22080 | IPServices | 12.4.15T: WebVPN stops working with TCP connection queue limit reached |
| CSCsl23788 | IPServices | Dlsw+ peer waits in AB_PENDING or WAIT_WR status with modular IOS |
| CSCsl31074 | IPServices | FA4 line protocol goes up and down when no cable is connected with dhcp |
| CSCsl43580 | IPServices | "standby delay minimum" produces  incorrect values while configuring |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl51945 | IPServices | HSRPv6: Config Sync and stanby resets with standby 1 ipv6 <> |
| CSCsl51982 | IPServices | nat_sanity:Traceroute test from outside to inside fails |
| CSCsl67168 | IPServices | HSRP should output state change log of both Active/Standby<->any |
| CSCsl72281 | IPServices | Interface-index in DHCP binding database changes after router reload |
| CSCsl74712 | IPServices | VRRP: Config Sync: vrrp 1 track 1 decrement 10 |
| CSCsl96370 | IPServices | CPU hog msg during interface reset for scaled hsrp config (debug enbld) |
| CSCsm34361 | IPServices | Required ports [TCP] are not shown in nmap package in PC |
| CSCsm35794 | IPServices | Ignoring Coup after changing HSRP active router's priority |
| CSCsm36745 | IPServices | Warning message for DNS-lookup when no DNS server present |
| CSCsm59037 | IPServices | no service dhcp command causes switch to reload |
| CSCsm70580 | IPServices | c2w2:ciscoFtpClientMIB: ftp_fs.proc extra processes can deadlock & crash |
| CSCsm71240 | IPServices | HSRP not replying to ARP after removing and changing hsrp groups |
| CSCsm79082 | IPServices | RP crash at dispatch_thread_pool when restarting tcp.proc |
| CSCsm87959 | IPServices | HSRP IPv6 becomes :: or unknown after changing interface IP addr |
| CSCsm92206 | IPServices | Router crashes when set the range of interfaces to default configs |
| CSCso04657 | IPServices | SSLVPN service stops accepting any new SSLVPN connections |
| CSCso17473 | IPServices | Stby reload continuously with HSRP: Grp 1 RF Encode data descriptor fail |
| CSCso30669 | IPServices | HA-6-INT_SSO_UNAWARE : While enabling VRRP-SSO onboard GE-interface |
| CSCso68344 | IPServices | Switch acting as DHCP server crashes on issuing no service dhcp command. |
| CSCso74843 | IPServices | stuck in ACTIVE-DRAIN state after 1 day of switchovers |
| CSCso91230 | IPServices | %LINK-2-INTVULN: errors with MLPPP and HWIC-4ESW |
| CSCso97695 | IPServices | backout CSCsm88549 and fix CSCsl48943 with proper fix |
| CSCsq06813 | IPServices | DHCPV6:No multiple RELEASE messages seen on client |
| CSCsq14698 | IPServices | crash when using nat with multicast traffic |
| CSCsq47043 | IPServices | Standby crashes when re-configuring "standby <group> ip" command |
| CSCsq48201 | IPServices | c7300:Bridge IRB-Router crash and traffic flow issue |
| CSCsq60504 | IPServices | Modular IOS Sup720: crashed with tcp timeout logs |
| CSCsq67478 | IPServices | SSH session hangs |
| CSCsq88779 | IPServices | Router fails to boot with overlap address |
| CSCsq90529 | IPServices | Issue with active ftp on the SXH1 |
| CSCsq92440 | IPServices | Router Crash with igmp static grp classmap for 10k grps on 10 subints |
| CSCsq97870 | IPServices | Router crash with 'show standby' if group deleted from 2nd terminal |
| CSCsr08771 | IPServices | Crash seen @ dhcpd_pool_nvgen and dhcpd_copy_bootfile |
| CSCsr18589 | IPServices | Due to SSO of the Backupswitch, VRRP is flapping |
| CSCsr27287 | IPServices | HSRP group get stuck in Init state after changing IP to secondary |
| CSCsr55990 | IPServices | HSRP mac dynamic on routed pseudowire after reload on active router |
| CSCsr60108 | IPServices | standby delay timer range changed from 0-10000 to 0-300 |

| Identifier | Technology | Description |
|---|---|---|
| CSCsr96468 | IPServices | Standby config accepted even when MAC reservation failed |
| CSCsu10108 | IPServices | TFTP Server function is not working in 7600 router |
| CSCsu21716 | IPServices | No unsolicited igmp report sent for mroute-proxy |
| CSCsu27843 | IPServices | SW crashed when removed "int vl" on which "ipv6 dhcp client pd" enabled |
| CSCsu56806 | IPServices | HSRPv6 configuration reappears after deleting/configuring SVI |
| CSCsu93374 | IPServices | After SSO standby router, client state doesn't follow master group state |
| CSCsv06608 | IPServices | SXP peering between cat6k with password none option is broken |
| CSCsg87930 | LAN | i82543 driver should not increase input queue drop counter |
| CSCsl54243 | LAN | 7600 SIP-400 crash after removing sub-ints; lc_deencap_dot1q_vlan |
| CSCsm02883 | LAN | MFR interfaces do not respond to SNMP after OIR |
| CSCsr76818 | LAN | input queue wedge on SP due to VTP packets |
| CSCsh33167 | LegacyProtocols | Dlsw transparent cache holds MAC address for disconnected circuit |
| CSCsi09051 | LegacyProtocols | Spurious Access seen with ipx routing |
| CSCsk94676 | LegacyProtocols | dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH |
| CSCsk98507 | LegacyProtocols | Device crash@novell_send_gen_rip_query . |
| CSCso09152 | LegacyProtocols | Slow leak in small buffers caused by CLS_CLOSE_STN |
| CSCeh97382 | Management | Device reset when polling IKE/IPSEC MIB |
| CSCsk38681 | Management | VS2: remote registry call messages ~ cdp2.iosproc:1 |
| CSCsk41552 | Management | T/B %SCHED-3-THRASHING of cdp2.iosproc process_wait_for_event |
| CSCsl64470 | Management | router reload with cns config notify |
| CSCsl68464 | Management | SNMP walk on .1.3.6.1.2.1.4.20.1.2 causes CPUHOG clearing tcp session |
| CSCsq52847 | Management | Connection establishment failed with the event agent |
| CSCsq79032 | Management | Excessive remote registry invocation on 'waiting_on_switchover' registry |
| CSCsq79132 | Management | Excessive remote registry invocation on 'proto_on_swidb' registry |
| CSCsq84595 | Management | high # of remote reg. invocation (35 rpc/sec) 'get_unidirectional_mode' |
| CSCsr93672 | Management | Native vlan is not getting displayed in "show cdp neighbors" output |
| CSCsv08562 | Management | IPv6 System crash on bootup with config saved,TB @ dispatch_thread_pool |
| CSCek72661 | MPLS | snmp context doesnt work with new VRF definition CLI. |
| CSCsd80349 | MPLS | Rainier:FRR is not successfully triggered on line prot down event on POS |
| CSCse23302 | MPLS | Staled LDP target session not removed after session flapping |
| CSCsh97826 | MPLS | NRT:6VPE:InterAS entry may not gt installed properly when nxthop is IPv4 |
| CSCsj21066 | MPLS | 6VPE: adding route-target to IPv6 AF causes IPv4 eBGP session to reset |
| CSCsj34456 | MPLS | LDP change by CSCsi69278 causes inconsistent mplsLdpEntityIndex value . |
| CSCsj50412 | MPLS | Improper handling of remote binding wrt route info |
| CSCsj98922 | MPLS | 6VPE - per vrf default route handling broken |
| CSCsk10104 | MPLS | NSE-150, MPLS TE tunnel does not come up after sh/nosh core interface |
| CSCsk15476 | MPLS | MPLS-TE auto-tunnel backup cannot protect primary nhop via L1L2 link |

| Identifier | Technology | Description |
|---|---|---|
| CSCsk42307 | MPLS | MPLS-TE CBTS: Sending out OSPF hellos over master tunnel . |
| CSCsk57114 | MPLS | CPUHOG process = SNMP ENGINE, PWMIB, GetNext of cpwVcMplsNonTeMappin |
| CSCsk62514 | MPLS | Parsing Configuration takes longer time on SUP720 with SRB image |
| CSCsl39233 | MPLS | eBGP in VRF-lite not working in images without MPLS . |
| CSCsl90265 | MPLS | CBTS member tunnels are not recovered after SSO switchover |
| CSCsm10306 | MPLS | CBTS master down by member path change causes unexpected traffic loss |
| CSCsm70668 | MPLS | OIR over E3:POS impacting complete Traffic with biscuit tunnel |
| CSCsm86236 | MPLS | Standby reload on reconfiguring address-family ipv4 under vrf definition |
| CSCso07411 | MPLS | Config-sync MCL due to ip ospf interface-retry 0 command getting added |
| CSCso21506 | MPLS | Import Map under vrf blocks bgp aggregate prefix |
| CSCso23419 | MPLS | CBTS master tun reported down for 10 sec after member tun comes up |
| CSCso51637 | MPLS | Crash on removing interface auto-template with 300 active tunnels |
| CSCso53377 | MPLS | All TE Lsps does not recover after SSO switchover |
| CSCsq02201 | MPLS | show run vrf does not display static route with track option |
| CSCsq46044 | MPLS | Error MFI_LABEL_BROKER-3-DELETE_MOI_FAIL and LSD_CLIENT-3-PCHUNK2 |
| CSCsq78822 | MPLS | Cannot clear specific LDP neighbor, when router-id not in bound address |
| CSCsq83958 | MPLS | 6VPE add remove VRFs crash at avl_balance_right avl_delete_recursive |
| CSCsq91960 | MPLS | failed to delete vrf when it is 32 characters long |
| CSCsq93004 | MPLS | Possible memory corruption with TE auto-tunnel primary and subinterface |
| CSCsr31401 | MPLS | mpls-layer tunnel int  not deregistered from snmp when tunnel deleted |
| CSCsr40433 | MPLS | mpls te - explicit path with loose nhops - re-optimization failure |
| CSCsr43164 | MPLS | FRR may not become ready after reoptimize backup tunnel |
| CSCsr50099 | MPLS | show ip explicit-paths command incorrectly displays source route type |
| CSCsu62667 | MPLS | LSP ID change after SSO due to failure in signalling recovered LSP |
| CSCek75931 | Multicast | LNS: %SYS-3-CPUHOG When sessions  have multicast |
| CSCsd14706 | Multicast | PIMV2 router send PIMV1 RP-reachable messages loading recieve router CPU |
| CSCsg95192 | Multicast | no ip rp-address <ACL name> causes an address error |
| CSCsg98535 | Multicast | IPv6: clear ipv6 pim topology with (S1,G30K) caused watchdog timeout |
| CSCsi59438 | Multicast | ip multicast limit rpf - fails to stop excessive groups from forming |
| CSCsj88725 | Multicast | Wrong (S,G) RPF after route change, no upstream join |
| CSCsk26429 | Multicast | Router configured for IGMP Proxy may not send IGMP Join |
| CSCsk45472 | Multicast | Bootstrap packets from non-RPF neighbour not dropped on MDT Tunnel |
| CSCsl10316 | Multicast | ipv6 pim join-prune-interval 10 sets the interval to 20 seconds . |
| CSCsl14450 | Multicast | Multicast traffic in Tunnel environments may cause router crash |
| CSCsl20158 | Multicast | SNMP:msdpPeer counters should be able to compare with CLI counters. |
| CSCsl92316 | Multicast | LNS: %SYS-3-CPUHOG when clear l2tp tunnel, sessions have multicast |
| CSCsm02687 | Multicast | 3725 router is crashing @oce_base_unlock,ipmulticast_les_fastswitch |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm17426 | Multicast | RP-bit not cleared on s,g; traffic outage for 4 minutes |
| CSCsm26466 | Multicast | Standby RP goes down with %MCASTRED-3-BULKACKTIME on active |
| CSCsm44620 | Multicast | Shutdown interface present in PIM interface list |
| CSCsm48322 | Multicast | IPv6 Multicast RP ignores embedded RP register messages |
| CSCsm53766 | Multicast | Reload due to Address Error with multicast configuration |
| CSCsm73602 | Multicast | "ip multicast boundary" makes "VTEMPLATE Backgr" consume much CPU usage |
| CSCsm77608 | Multicast | IP Multicast packets are Process switched. |
| CSCso67195 | Multicast | Memory Corruption Crash with PIM and ACL Logging enabled |
| CSCsq09962 | Multicast | 7600 : crash at "pim_proxy_empty_rd" |
| CSCsq14151 | Multicast | RPF of (S,G) is set to NULL, When (S, G, R) entry is convered to (S, G) |
| CSCsq44925 | Multicast | CSCsi47802 need to be modified |
| CSCsr00815 | Multicast | IPv6 PIM Assert winner remains in Incoming interface: Null state |
| CSCsr09312 | Multicast | crash when doing mrm stop |
| CSCsr15478 | Multicast | Input Queue Wedging |
| CSCsr36971 | Multicast | Memory Leak @ PIM process |
| CSCsr49316 | Multicast | Crash ipv6_static_route_find after configured & executed show ipv6 rpf x |
| CSCsr82895 | Multicast | watchdog timeout : RP Crash @ igmp_rejoin_groups during RP Switchover |
| CSCsu02051 | Multicast | S,G expiry timer change is not allowed in Whitney1 |
| CSCsu27888 | Multicast | igmpv3 reports are getting discarded |
| CSCsu71983 | Multicast | Memory Leak @ PIM process |
| CSCsu95080 | Multicast | mld_processs block forever in the init_process when parsing config |
| CSCec08614 | platform-12000 | Incrementing spurious accesses at srpmib_interface_lookup_long_int |
| CSCse40966 | PPP | MLP links down after SSO switchover if aaa new-model cfged |
| CSCsi43652 | PPP | PPP: ISSU negotiation should be skipped if standby is incompatible |
| CSCsl27840 | PPP | Router may Crash / Hang, Module Reset @ Shut ATM member + MLPOA |
| CSCsm41129 | PPP | SRB3:140DLFI bundles with qos-Flapping, pkts choke RP as RP does fragmt |
| CSCso28309 | PPP | ping fails while testing pppas feature |
| CSCsq37078 | PPP | Input errors incrementing on Multilink 5 in admin down state |
| CSCsq55691 | PPP | DLFIoATM QoS doesn't work after physical interface shut/no shut |
| CSCef63607 | QoS | Crashes seen during boot if ATM WIC is installed & NAT on int config |
| CSCek52651 | QoS | Traffic shaping broken and drop rate counters are junk |
| CSCek63203 | QoS | CEOP:VH:Ctrl+C while display show policy int cause console freeze |
| CSCek75808 | QoS | MF: Crash observed at qos_show_policymap_interface_all |
| CSCsg18894 | QoS | Queue-limit command should be allowed in conjunction with priority |
| CSCsh67875 | QoS | support for multi-line policer broken |
| CSCsi73132 | QoS | Multicast DSCP value not copied to PIM-SM RP-register packet |
| CSCsj60212 | QoS | sip200: Traceback@reg_invoke_qoscli_inform_features with qos config |

| Identifier | Technology | Description |
|---|---|---|
| CSCsk06872 | QoS | SIP-600 QoS : Unsupported configuration is accepted |
| CSCsk63794 | QoS | FlexWAN WS-X6582-2PA + T3+ Serial PA may crash/reload |
| CSCsl62963 | QoS | Router Crashes, Reconfigure a Policy -af_police_remove_coloraware |
| CSCsm00570 | QoS | cwpa2 crashes at hqf_cwpa_pak_enqueue_local |
| CSCsm38142 | QoS | 7600 L2WAN SYSTEST: Memory leaking fib_rp_process_feature_classify_stats |
| CSCsm49062 | QoS | cwan2: show queueing interface reports double count for wfq drops |
| CSCsm87634 | QoS | Incorrect burst values seen on policy with multiple policers. |
| CSCsm93513 | QoS | QoS: "queue-limit" config not allowed in dual-level priority queuing |
| CSCso27913 | QoS | Router Crashed, Remove / Modify Conform&Exceed Color class - af_policer_ |
| CSCso50587 | QoS | FRR protection is failing after no shutdown backup tunnel |
| CSCso57695 | QoS | policy-map add/removal from interface crashes router. |
| CSCsq37520 | QoS | RP crashes when child-policy added to 1000s of targets |
| CSCsq43678 | QoS | Address error on output policing packet that was not classified |
| CSCsr44492 | QoS | To add user-defined classes restriction at proper place |
| CSCsu03813 | QoS | Upgrading from rockies to w2 deletes the police action from pmap |
| CSCdy87411 | Routing | BGP:Need to delete one list of ip extcommunity-list entries |
| CSCeg25475 | Routing | Distribute-list configured in ipv4 acts in vpnv4 address-family |
| CSCei25699 | Routing | cIpAddressIfIndex of CISCO-IETF-IP-MIB returns 0 value. |
| CSCek36995 | Routing | 0.0.0.0 default route increasing on rip DB with object tracking |
| CSCek51676 | Routing | boomclone:deleting SVI crash RP and standby does not take over |
| CSCek55562 | Routing | Tracebacks at topo_db_lookup_by_vrfid due to CPUHOG |
| CSCek68270 | Routing | router crashed at eigrp_ipv4_rib_rdbupdate |
| CSCek78031 | Routing | Tunnel VRF:Rx-rate is 0.Traffic does not reach the destination port |
| CSCsc40107 | Routing | command clear ip bgp vrf VRF_Name flap-statistics not working |
| CSCsc96014 | Routing | EIGRP neighbors from primary add space deleted when sec add removed |
| CSCsd68016 | Routing | ip summary-address rip 0.0.0.0 0.0.0.0 sends out default with metric 16 |
| CSCsd98686 | Routing | %XDR-6-CLIENTISSUBADTXTFM: Failed to xmit_transform message . |
| CSCse00039 | Routing | ipv4 prefixes not advertised to EBGP peers |
| CSCse15634 | Routing | neighbor default-originate doesn't work in address-family ipv4 multicast |
| CSCse26506 | Routing | PRE2: BGP CPUHOG when OIR ATM interface -- rt_walktree_cond |
| CSCse47937 | Routing | ICMP unreachables sourced by IOS may contain buffer data |
| CSCse65277 | Routing | MU:default isis metric maximum returns parser error |
| CSCse97209 | Routing | Outbound route-map with continue option sets incorrect std communities |
| CSCse99913 | Routing | Implementation of SYSLOG message for peer reset due to lack of UPDATE |
| CSCsf06946 | Routing | Removing loopback interface causes continuous standby RP reloading |
| CSCsf11076 | Routing | Static route to Null0 with net defined in process not added to topology |
| CSCsg27697 | Routing | router rip AF ipv4 causes standby PRE reset continuously due to BEM erro |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg49166 | Routing | EIGRP fails to converge with 1100 neighbors on FR point to point PVCs |
| CSCsg68717 | Routing | A weird behavior in maxpath configuration in ebgp+ibgp case |
| CSCsg80259 | Routing | BGP Routes do not re-populate follwing reload of Secodary Route Reflect |
| CSCsg90755 | Routing | Standby keeps reloading due to PRC mismatch in IPv4 MDT AF config sync |
| CSCsg92473 | Routing | Switch crashes - IPV6 reflexive acl scalability test |
| CSCsh12493 | Routing | BGP overlapping VRF route not installed in RIB after add/del of VRF |
| CSCsh20497 | Routing | EIGRP IPv6 rtr crashes when config eigrp on serial int (3k/4k port) |
| CSCsh26706 | Routing | ab76:ESM2 TB point to fibidb_decode_update&bitlist_validbit after reload |
| CSCsh34417 | Routing | BGP Distance not updated following failover to a path with a greater dis |
| CSCsh52567 | Routing | MF:Switch Asserts when setting the AS-Path with BGP Route-Map Continue |
| CSCsh54797 | Routing | high CPU in collection process after bringing up pppoe sessions twice . |
| CSCsh56042 | Routing | sham-link goes down when TYPE-5 for SL neighbor address is flushed |
| CSCsh79933 | Routing | BFD does not notify EIGRP of subsequent bfd session failures |
| CSCsh82722 | Routing | RIP routes removed from rip db but stuck in vrf routing table |
| CSCsh82953 | Routing | EIGRP pece routes missing extcomm attrs after redistribution to BGP . |
| CSCsh86480 | Routing | NRT: traceback seen bgp_atf_error |
| CSCsh92749 | Routing | ISIS: ADJ del triggers both LSP and SPF |
| CSCsh96955 | Routing | IPv6 routes learned from eBGP multihop neighbor not installed in RIB |
| CSCsi07687 | Routing | Self ping to SVI fails when vlan configs are removed and re-applied. |
| CSCsi07822 | Routing | 6VPE:FIB cannot resolve chain on link flap with eBGP MH Ldsharing in VRF |
| CSCsi12104 | Routing | ipv6_nd_timer:After the shutdown of active router int router is crashing |
| CSCsi14346 | Routing | EIGRP: neighbor command missing in VRF. |
| CSCsi29163 | Routing | BGP: Network statement shows different in the configuration |
| CSCsi34354 | Routing | CET: ATFv4: Assertion tracebacks observed |
| CSCsi51431 | Routing | JQL:SIERRA:SP HighCPU/LCboot up fail with largeACL cfg after sw reload |
| CSCsi53802 | Routing | Change in prefix-list used by vrf import/export map not processed by BGP |
| CSCsi58867 | Routing | CPUHOG After show ip route static or show ip route connected |
| CSCsi68795 | Routing | PE wrongly assigns local label to a vpnv4 confederation prefix |
| CSCsi70484 | Routing | OSPF SPF running constantly if LSID conflicts & prefix filter used. |
| CSCsi83521 | Routing | CLI:Router Crashes after executing sequence of permit commands. |
| CSCsi87894 | Routing | RIP advertise default route after 'no default-information originate' |
| CSCsi97315 | Routing | bfd dereg under peer-grp and peer-session broke |
| CSCsi98730 | Routing | CEF/BGP table MPLS label mismatch in IOS 12.4(6)T5 |
| CSCsj03030 | Routing | Chunk memory allocated from the chunk battr_chunks is not freed |
| CSCsj13911 | Routing | Cat3750:EIGRP does not receive reply for query between some Vlan |
| CSCsj21785 | Routing | TE tunnel does not reoptimize after mtu change |
| CSCsj34688 | Routing | AAA: adding static route cfg does not trigger acct msg to tacacs server |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj37111 | Routing | IPv4 inconsistencies & %FIB-4-FIBXDRINV upon reset LC |
| CSCsj39016 | Routing | warn_assert failed: ../fib/fib_table.c:2947 tal_tree_get_item_count_nonf |
| CSCsj39243 | Routing | Issues in IPV4 with summary statement after moving interface to vrf |
| CSCsj40173 | Routing | HSRPv2 Ping IPv6 link-local not recognize the source address |
| CSCsj45837 | Routing | BGP with auto-summary stops advertising classful network if subnet flaps |
| CSCsj48450 | Routing | When configured ICMP code 251-255 on ACL, ACL is not properly configured |
| CSCsj56281 | Routing | BGP inherit peer-policy not working after router reload |
| CSCsj71764 | Routing | incorrect ARP resolution when going through MPLS VPN |
| CSCsj78403 | Routing | clear ip bgp  causes crash to RR client with conditional route injection |
| CSCsj89636 | Routing | isis convergance time delay with equal paths |
| CSCsj94697 | Routing | Show ip bgp vpnv4 update-group summ causes high cpu |
| CSCsk04287 | Routing | Spurious memory access at 0x9DA3070 reading 0xC |
| CSCsk14365 | Routing | show command to display recently changed bgp prefixes |
| CSCsk15805 | Routing | static route not removed after TE tunnel shut |
| CSCsk27077 | Routing | router crash observed while clearing  virtual access interface |
| CSCsk34344 | Routing | Wrong share-count 1:10 via confed-external BGP peers using dmzlink-bw |
| CSCsk35688 | Routing | Aggregate routes not processed if child routes are deleted pre-maturely |
| CSCsk37659 | Routing | Vrf route table does not get updated once pppox sessions are up. |
| CSCsk38877 | Routing | PE_PUNT_UNRECOGNIZED should be an OUTPUT_FEATURE . |
| CSCsk48525 | Routing | Make ipv4fib global feature message ISSU compliant . |
| CSCsk54092 | Routing | Type 3 LSA's not flushed when network command is removed . |
| CSCsk56663 | Routing | BGP RFC3107 Withdrawn route should have label 0x800000 and had 800001 . |
| CSCsk63429 | Routing | SRB2: High CPU utilization due to MPLS IPRM process after linecard reset |
| CSCsk65460 | Routing | MVPN: mcast-FS fails on decapPE |
| CSCsk71117 | Routing | Traceback with %XDR-6-XDRDISABLEREQUEST: after loadversion |
| CSCsk78854 | Routing | Make ipv6fib global feature message ISSU compliant . |
| CSCsk79113 | Routing | memory leak in VTEMPLATE Background if standby dissapears |
| CSCsk80250 | Routing | BGP has to handle the return value REXP_DONTKNOW of regexec_hybrid |
| CSCsk82988 | Routing | ttl-security next hop inaccessible when peering to loopback |
| CSCsk83038 | Routing | During the ISSU runversion vacl packets switched in SW . |
| CSCsk84653 | Routing | EIGRP variance unequal cost load balance routes get stuck . |
| CSCsk86150 | Routing | w/ BGP auto-summary enabled, networks are lost from BGP after EIGRP flap |
| CSCsk86476 | Routing | OSPF fails in MTU-mismatch setup when mtu-ignore is configured |
| CSCsk89546 | Routing | RIB and FIB not updated after shut TE LB path |
| CSCsk95829 | Routing | TE Tunnel intf is removed from routing table after rapid shut/no shut |
| CSCsk95969 | Routing | mfibv6: Crash in ipv6_pdb_find_ipdb while configuring ipv6 address |
| CSCsl04835 | Routing | BGP conditional route injection not removing routes from iBGP peers |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl06336 | Routing | removing 'maximum-paths import 6' causes duplicate paths in VRF table |
| CSCsl07297 | Routing | SXF11: BGP "no neighbor" command caused Address Error exception . |
| CSCsl13950 | Routing | VS2:XDR_LC traceback seen on Standby-RP on bootup . |
| CSCsl15208 | Routing | OSPF DCbitless LSA count goes negative with OSPF flood reduction enabled |
| CSCsl20133 | Routing | PE-CE: remote vpn routes with SoO not advertised to CE |
| CSCsl20856 | Routing | standby HSRP flaps with ospf mib polling/aggressive timers/nostandby sso |
| CSCsl28278 | Routing | OSPF-Route/CEF entry lost after SSO on the neighbor |
| CSCsl30331 | Routing | Prefixes permitted despite the deny action on route-map continue |
| CSCsl31627 | Routing | vrf aware NHRP/mGRE, Crash in rn_walktree_blocking while removingtnl |
| CSCsl32318 | Routing | OSPF: new fix for CSCsk36324 SPF loop |
| CSCsl33632 | Routing | Router crash at vrf_interface_associate when vrf is unconfigured . |
| CSCsl47915 | Routing | Redistribution of ospf in rip with prefix-list not working properly |
| CSCsl48075 | Routing | Floating static route behaves incorrectly in 6vPE |
| CSCsl49628 | Routing | VRF is not getting deleted in 'sh vrf' output |
| CSCsl50271 | Routing | Enhancement is needed in OSPF to avoid suspend |
| CSCsl51616 | Routing | v6-vrf-lite config doesn't sync properly with standby |
| CSCsl52594 | Routing | Cannot ping ipv6 loopback addr (No valid source address for destination) |
| CSCsl56547 | Routing | sh mls cef ipv6 vrf <id> for 6VPE  says VRF ids does not exist |
| CSCsl56914 | Routing | OSPFv3 router LSA stuck in retransmit |
| CSCsl57457 | Routing | ISIS NSF switchover failure - similar to CSCsl28278 |
| CSCsl62076 | Routing | Router crashed when configuring IPv6 RIP |
| CSCsl63869 | Routing | %DUAL-3-INTERNAL: EIGRP-IPX: PDM Internal Error while processing dndb |
| CSCsl69845 | Routing | VPDN/MPLS : Interface counter not incremented by labeled packets |
| CSCsl71540 | Routing | Router crash after using cmd 'sh ip bgp x.x.x.x [bestpath |
| CSCsl72774 | Routing | Memory leak in CEF consistency checker |
| CSCsl80887 | Routing | Traceback @ rip_sendupdate_subr when update timer set to '0' |
| CSCsl83415 | Routing | Rtr crash in show cmd: new updgrp add enlarges Nbr bitfield size for Tbl |
| CSCsl84712 | Routing | Error- %OSPF-4-FLOOD_WAR: Process 123 re-originates LSA ID 10.55.122.148 |
| CSCsl85391 | Routing | TE Tunnel remains down after remove/add IP address |
| CSCsl92283 | Routing | Unable to add into routing table if static route use interface + gateway |
| CSCsl94410 | Routing | Back out the CSCsj17879 for all non ERF branch |
| CSCsl95609 | Routing | Alignment TBs@bgp_ipv6_mpath_statechng_inprocess on del/add 6VPE vrf |
| CSCsl96254 | Routing | EIGRP distribute-list not checked if intf distribute-list permits route |
| CSCsm04442 | Routing | Router crash at rip_find_sum_idb |
| CSCsm05082 | Routing | BGP Dampening penalty not decaying on frqnt 'sh ip bgp v all' [dampening |
| CSCsm10603 | Routing | L2tp sessions were getting flapped |
| CSCsm17899 | Routing | OSPF routing loop when using Virtual-Link |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm23764 | Routing | CEF RF progression error if RRP reloads mid CEF sync |
| CSCsm26130 | Routing | BGP with auto-summary not injecting locally orig. route into BGP table |
| CSCsm26968 | Routing | ipv4 prefix added to routing table in error next hop int ipv4 disabled |
| CSCsm27958 | Routing | Control Plane interface in OSPF interface added preventing SSO oper |
| CSCsm27979 | Routing | router may crash for "address error exception" doing sh ip route vrf |
| CSCsm30569 | Routing | CEF path fragmentation broken for static IPSec VTI |
| CSCsm36500 | Routing | TB@adj_add w/ %ADJ-3-NOFIBIDB: CEF Interface not found msg on SPA OIR |
| CSCsm39159 | Routing | ARP HA cpu hog on stby while bringing up stby with large arp tables |
| CSCsm39308 | Routing | Null Pointer Read condition detected in "clns_find_router_name()" |
| CSCsm39730 | Routing | BGP churn: VRF route version number keeps increasing |
| CSCsm41873 | Routing | MCP: Router crashes while unconfiguring the <ip vrf "vrf name"> |
| CSCsm43938 | Routing | stby resets when large config/arp table to sync over to it |
| CSCsm45634 | Routing | BGP VPNv4 route is not actived immediately after receving update |
| CSCsm47111 | Routing | FIB: Accessing freed memory while dequeuing |
| CSCsm49143 | Routing | 6VPE: IPv6 PING is broken in whitney2 SX142 with VRF and source address |
| CSCsm50741 | Routing | Removal of DCbitless LSA causes problems |
| CSCsm57494 | Routing | BGP update is not sent after reloading opposite router |
| CSCsm64516 | Routing | OSPF MD5 Key Does Not Accept Whitespace Character |
| CSCsm64643 | Routing | IPv6 passive interface address not in the isis database |
| CSCsm72604 | Routing | OSPF remaining summary route when dual OSPF process redistributing |
| CSCsm91801 | Routing | ASBR not updating metric in LSA-5 redistributing from 2-nd OSPF process |
| CSCsm95129 | Routing | "no ip next-hop-self eigrp" not working when redistribute from BGP |
| CSCsm96785 | Routing | "nsf cisco" under router ospf config does not work, but "nsf ietf" works |
| CSCsm96901 | Routing | Unable to ping between vrfs through transparent bridge |
| CSCsm98767 | Routing | show ip bgp neighbor does not relfect actual sent/received prefix number |
| CSCso00383 | Routing | MVPN: New style PE doesn't send  RD Type 2 MDT update |
| CSCso07371 | Routing | SCHED-7-WATCH: Attempt to set uninitialized watched boolean in pfxlist |
| CSCso07520 | Routing | MCP:OSPFv3 BFD Link-Local peers flap during RP/SSO switchover |
| CSCso08786 | Routing | Standby reloads due to config sync failure on inherit peer-policy cmd. |
| CSCso09977 | Routing | EIGRP IPv6: include-connected option does not work for EIGRP routes. |
| CSCso12305 | Routing | cfc_dev: Missing IPv6 prefixes on unixrp found by full-scan-rib-ios cker |
| CSCso14177 | Routing | EIGRP offset-list with interface modifier does not send correct metric |
| CSCso14979 | Routing | Notify platforms when FIB disables dCEF for a linecard |
| CSCso15740 | Routing | 'set metric' clause' in continue route-map sequence does not set metric |
| CSCso22098 | Routing | OSPF down on RPR+ switchover on core router |
| CSCso22883 | Routing | Passive-interface command applied to all address-families |
| CSCso25823 | Routing | Router crashes when mpls ip command is issued on 12.2(32.8.11)SR129 imag |

| Identifier | Technology | Description |
|---|---|---|
| CSCso30199 | Routing | ISIS topology broken after a force-switchover when ispf is enabled |
| CSCso38444 | Routing | Change of OSPF network type may break MPLS TE Topology database |
| CSCso39597 | Routing | StbyRP crashed @ bgp_vpnv4_bulk_sync_mpls_lbl_binding during bulk sync |
| CSCso40442 | Routing | BGP sessions Idle after switchover from RPR+ mode |
| CSCso51519 | Routing | Paths with same Nexthop selected as multipaths in some sequence |
| CSCso52344 | Routing | Inconsistent fib entry for 224.0.0.0/4, drop vs multicast oce on RP/LC |
| CSCso54167 | Routing | BGP peer stuck with table version 0 |
| CSCso55151 | Routing | ADJ not freeing memory under IPv6 ND stress test |
| CSCso62166 | Routing | Crash @ bgp_netlist_validate when ibgp established with metric |
| CSCso63693 | Routing | ISIS: Maximum circuit limit (255) has reached with passive-interface def |
| CSCso64274 | Routing | 0.0.0.0/0 redistributed entry not removed RIP DB after deleting command |
| CSCso65266 | Routing | Memory leak at BGP Router on 12.0(32)Sy4 |
| CSCso67141 | Routing | BGP routes are not removed when peer goes down |
| CSCso67850 | Routing | CMTS crashes in ipv6_nd_prefix_get_addr_sb |
| CSCso73076 | Routing | can not delete ACE enties in ACL |
| CSCso76661 | Routing | DHCPv6 PD not working after interface flap |
| CSCso80951 | Routing | BGP peers with same policy fall into different update-group with SOO |
| CSCso87916 | Routing | IPv6 RIP Router crashed,TB @ ipv6_rip_idb_down |
| CSCso89675 | Routing | Device crash @  ip2access_add_pbacl_item with largre PBACL configuration |
| CSCso93535 | Routing | Upon removing a VRF, BGP route timers in other VRF's get reset |
| CSCso98964 | Routing | EIGRP authentication not working for long key-strings |
| CSCsq02587 | Routing | Tunnel not coming up in EoMPLS with mpls TE case |
| CSCsq05602 | Routing | TE tunnels are down but still show in the forwarding table |
| CSCsq13111 | Routing | 7609s vlan traffic reporting |
| CSCsq13938 | Routing | reload on 'show ip bgp vpnv4' when import src delinked by BGP deconfig |
| CSCsq16611 | Routing | ipv6 packets are process switched instead of cef-switching. |
| CSCsq24935 | Routing | Switch crash due to unsupported bgp/ipv6  command |
| CSCsq26684 | Routing | ipv6 nd prefix CLI  should not update RIB |
| CSCsq29052 | Routing | Ping fails on applying ip unnumbered configs in mpls oam |
| CSCsq38431 | Routing | OSPF "summary address" is executed, even if subnet is becoming small |
| CSCsq38703 | Routing | BGP route still present on remote PE even after deleting  the VRF |
| CSCsq40845 | Routing | C2W2: standby reloads while unconfiguring ipv6 access-list with 080521 |
| CSCsq43831 | Routing | Stack overflow due to recursion in FIB |
| CSCsq44052 | Routing | ISIS: Unable to configure "is-type level-1" |
| CSCsq45082 | Routing | ip route with associated track/sla gets removed when track is still up |
| CSCsq49201 | Routing | Password in BGP peer-session template not inherited |
| CSCsq58164 | Routing | %IPV6-3-RIB address cannot be deleted when removing address from VRF RIB |

| Identifier | Technology | Description |
|---|---|---|
| CSCsq62703 | Routing | Router crashed with TLB (load or instruction fetch) exception |
| CSCsq75944 | Routing | crashes in ipflow_ager, ipflow_sub functions, ipflow_periodic |
| CSCsq86192 | Routing | dmzlink-bw not propagated after inheritance has been configured |
| CSCsq97517 | Routing | C2W2: Mago: CEF on RP is not in sync with SP after reboot. |
| CSCsq99447 | Routing | When BFD/ EIGRP configured in more than 32 vrf BFD does not come up |
| CSCsr07262 | Routing | IPv6 ND response is very slow(>10s) during RP switchover |
| CSCsr08468 | Routing | some extarnal OSPF routes are unable to be installed into Routing Table |
| CSCsr20566 | Routing | interface permanently dampened from routing perspective / STUCKTMR |
| CSCsr27794 | Routing | BGP updates stuck during peer flap |
| CSCsr30406 | Routing | no capability opaque w/o nsf ietf helper disable cause err msg |
| CSCsr41079 | Routing | %CHKPT-4-NOMESSAGE: Message is NULL, (Cannot get data ptr) |
| CSCsr45653 | Routing | Prefixes not deleted by CEF distribution broker |
| CSCsr55922 | Routing | router id is not correctly set in EIGRP ipv6 process |
| CSCsr67177 | Routing | Router with IPv6 OSPF crashes on reloading |
| CSCsr67562 | Routing | Support for running ispf with nodes having overload bit configured |
| CSCsr67863 | Routing | c2w2:TB seen in RPR-->ISSU-3-NOT_FIND_MSG_SES: Can not find message sess |
| CSCsr74295 | Routing | static route to mlppp not in rib |
| CSCsr83062 | Routing | IOSD crash at ipv6_show_interface when doing "show ipv6 interface" |
| CSCsr83639 | Routing | Bus error crash when removing BGP configuration |
| CSCsr86174 | Routing | aggregate-address under address-family does not appear in conf |
| CSCsr90248 | Routing | "aggregate-address advertise-map" not updated dynamically |
| CSCsr96042 | Routing | ASR: IOSD crashes at bgp_vpn_import_walker while unconfiguring vrf |
| CSCsu03167 | Routing | SXF15: IPv4/v6 BGP routes not cleared when source routes is gone |
| CSCsu12040 | Routing | PE with CsC configuration sends wrong labels to SPE |
| CSCsu24087 | Routing | Cisco7609 crashes after "clear ip bgp neighbor x.x.x.x soft in" |
| CSCsu31954 | Routing | Router crash when fragmenting packets with netflow |
| CSCsu36709 | Routing | Unable to boot IOS image on PE (vrf-enabled) router - software fault |
| CSCsu37200 | Routing | %SYS-3-BADTREEPARAM generated while aging DNA lsa type-11 |
| CSCeh98154 | Security | High Cpu when using show processes cpu monitor through SSH |
| CSCin91851 | Security | Support keyboard-interactive authentication method |
| CSCir01449 | Security | Sync damage of CSCin74155 fix |
| CSCsb58633 | Security | SCP server gives files with invalid checksum on some router platforms |
| CSCsb80803 | Security | SSH Process: SCHED-3-UNEXPECTEDEVENT error message |
| CSCsd02612 | Security | Failed Secure copy (due to exec privilige) not returning console prompt |
| CSCsd30932 | Security | CLI: router reload on bad refcount error during CA trust point config |
| CSCsd35474 | Security | router crashed during the capf upgrade |
| CSCsd81870 | Security | Teraterm + TTSSH2 does not work in SSH Ver.2 |

| Identifier | Technology | Description |
|---|---|---|
| CSCsf15428 | Security | Config change before Phase-2 rekeying results in SA lifetime mismatch |
| CSCsf17406 | Security | Large CRLs can cause memory leaks |
| CSCsg48392 | Security | Resuming SSH Session Fails After Disconnecting Another One (Not Console) |
| CSCsh54862 | Security | MPLS TE Tunnel Up by no shut without RSVP signalling completed |
| CSCsh72664 | Security | DMVPN: OSPF neighbor flap and traceback @ tunnel_oqueue. . |
| CSCsi50499 | Security | When aaa cmd author is enabled, SCP fails and tracebacks appear |
| CSCsi83287 | Security | %ALIGN-3-SPURIOUS T/B ipv6fib_gre_ipv6 after packet decap |
| CSCsj45031 | Security | Cat6k unable to SCP files from Tectia ssh server |
| CSCsk10376 | Security | MPLSoGRE EXP to external TOS not copied for locally generated packets |
| CSCsk43745 | Security | IP multicast fast  switching flag does not match expected value |
| CSCsk64898 | Security | NAT-PT is broken for ipv6ip tunnel traffic terminated on HSRP IP address |
| CSCsk75078 | Security | rcv client_input_channel_req: channel 0: unknown channel |
| CSCsl03084 | Security | 7600 SSH issues with privilege levels |
| CSCsl13561 | Security | Enhanced EzVPN no longer passes traffic |
| CSCsl43546 | Security | 6vPEoGRE :- mls cef programming incorrect on SIP600 after reset |
| CSCsl61311 | Security | New SSH sessions with RSA key sometimes fails after changing  hostname |
| CSCsl98498 | Security | Tunnel int is going down with  mode ipip decapsulate-any |
| CSCsm55629 | Security | Syslog for SSH returns NO username |
| CSCsm57122 | Security | Scp and ssh failing with certain ssh clients |
| CSCsm70913 | Security | UDLR: not able to clear portchannel config from the tunnel after del/add |
| CSCso48959 | Security | user not reported by "login on-success log" feature for SSH logins |
| CSCso64607 | Security | Router Crashes when no ip vrf <vrf> |
| CSCso67083 | Security | IOS crypto ACL does not support pattern matching (discontiguous subnets) |
| CSCso73533 | Security | %ALIGN-3-TRACE traceback seen @ ipv6_init_header |
| CSCsq14031 | Security | Ping fails through crypto tunnel on Full Service Branch testbed |
| CSCsq58748 | Security | IPSEC: IKMP process can get blocked by some PKI  OCSP requests |
| CSCsq60016 | Security | Router crashes when entering a long RSA key string |
| CSCsr55713 | Security | DMA Issue:Router crashed while doing ISATAP Tunnel Interoperability test |
| CSCsr85093 | Security | SXF15: SSH session fails withRSA signature verification failed after SSO |
| CSCdu70318 | Cisco IOS | Feature Request: VRF-lite PBR |
| CSCeb69473 | Cisco IOS | connect '/terminal-type' command memory corruption |
| CSCed88426 | Cisco IOS | Extended acl breaks on first switchover (Ctrl-C not synced to stdby) |
| CSCee25454 | Cisco IOS | SADB peering process leaks memory after overnight test |
| CSCeg35237 | Cisco IOS | Watchdog crash after sh crypto session |
| CSCeh08262 | Cisco IOS | Show tech SP output should honor redirect applied |
| CSCeh42472 | Cisco IOS | Standby RSP doesnt boot because of image uncompression failures |
| CSCeh52674 | Cisco IOS | no snmp-server host command will not remove entry from config |

| Identifier | Technology | Description |
|---|---|---|
| CSCeh96798 | Cisco IOS | sh mpls forward reporting none for Outgoing interface |
| CSCei52830 | Cisco IOS | Banner command sync is broken by CSCin86483 . |
| CSCei67734 | Cisco IOS | New RF state required for C10K Security ACL/Policy Map compiling |
| CSCej77184 | Cisco IOS | %LSD-4-LABEL_RESOURCE:label exhausted while sso switchover |
| CSCek35122 | Cisco IOS | Wrong statistics on input subinterface vlan counters for EoMPLS |
| CSCek37984 | Cisco IOS | Inconsistent BERT behaviour observed on TE1 SPA |
| CSCek39284 | Cisco IOS | fastethernet0/0/0 intermittently fails after switchover |
| CSCek40773 | Cisco IOS | CE-CE connectivity broken on MPLS VPN with GRE tunnel in VPN core |
| CSCek50172 | Cisco IOS | %SYS-3-TIMERNEG: Cannot start timer with negative set |
| CSCek63963 | Cisco IOS | EEM2.4:Getting the traceback when configuring rate based interfED |
| CSCek66142 | Cisco IOS | %SCHED-3-SEMLOCKED: rf proxy rp agent attempted to lock a semaphore |
| CSCek66877 | Cisco IOS | %XDR_SP-STDBY-6-CLIENTISSU_BLOCKED: XDR client lte broker cannotSync |
| CSCek67054 | Cisco IOS | ISSU Rollback timer should not wait for stdby in Hot if HA mode RPR |
| CSCek69134 | Cisco IOS | AB76:ESM20G MPB-E:RP hangs,CPU at 100% with default int on 8K EVC |
| CSCek71816 | Cisco IOS | CE-CE ping fail after restore ASBR-PE vrf |
| CSCek73818 | Cisco IOS | Router crash when issue mpls oam echo revision command on 7600 HA |
| CSCek75082 | Cisco IOS | Router crashes while unconfiguring channel-group |
| CSCek75768 | Cisco IOS | Ensure EEM policies are registered correctly through ssh. |
| CSCek76062 | Cisco IOS | Router crashed @ validmem_complete_interrupt . |
| CSCek77996 | Cisco IOS | High CPU caused by data traffic with crypto map in crypto connect mode |
| CSCek78653 | Cisco IOS | Cannot bring up PPTP sessions Due to FM Segment initialize failure |
| CSCek78874 | Cisco IOS | KMI:Out of order deletes cause sync issues |
| CSCin67287 | Cisco IOS | NxDS0 BERT capability on PA-MC-8TE1+ |
| CSCir00379 | Cisco IOS | NAD supplies old state attribute to ACS while sending new EAPID resp |
| CSCsa96960 | Cisco IOS | ip ttl expired lsp ping pkts shouldn'tt be transited by MFI process sw |
| CSCsb18498 | Cisco IOS | SNMP polling broken in cat6k SXE1 image |
| CSCsb57042 | Cisco IOS | %SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs |
| CSCsb87956 | Cisco IOS | loop  in the state  IKE_CONFIG_MODE |
| CSCsb92711 | Cisco IOS | HA: %ISSU-3-ERP_AGENT:req_msg is NULL traceback during slave boots up. |
| CSCsc05894 | Cisco IOS | Issue with IP MTU for IPSec VTI |
| CSCsc21582 | Cisco IOS | show crypto isakmp peer shows no output |
| CSCsc24015 | Cisco IOS | Parser loops infinitely for match route-type [ext |
| CSCsc59190 | Cisco IOS | %PM-STDBY-4-INT_FAILUP: fa4/3 failed to come up message after switchover |
| CSCsc85962 | Cisco IOS | Replaying Main Mode packet causing IKE SA deletion |
| CSCsd02012 | Cisco IOS | CEF data mismatch between RIP & VIP |
| CSCsd04608 | Cisco IOS | MQC-IPHC: Router crashed while testing mqc-iphc test |
| CSCsd08411 | Cisco IOS | EEM Tcl policy execution delayed relative to config size |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd09324 | Cisco IOS | IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP shown on stby RP when reload rtr |
| CSCsd47734 | Cisco IOS | Additional memory leak fixes by ActiveState |
| CSCsd48814 | Cisco IOS | Unable to start an SSH session from tclsh mode on the router |
| CSCsd69625 | Cisco IOS | EZVPN:IOS C876 Client can't connect to ASA using digi certs and noXauth |
| CSCsd70321 | Cisco IOS | Resetting a line card and an sso right after that - traffic gets dropped |
| CSCsd76111 | Cisco IOS | dot1x:%SM-4-BADEVENT cause by 'authTimeout' |
| CSCsd82457 | Cisco IOS | EOU Policy can't exempt Cisco 7935 Conference Station & Wireless phones |
| CSCsd87313 | Cisco IOS | ip cef load-shar algorithm universal not consistent between stack member |
| CSCsd98852 | Cisco IOS | EEM does not allow read from stdin |
| CSCse12518 | Cisco IOS | MET optimized update can cause blackholing and duplicates |
| CSCse15947 | Cisco IOS | 20 seconds of traffic loss after test crash 9 on active SP |
| CSCse16923 | Cisco IOS | 5850: IOS upgrade issue in handover split mode |
| CSCse31572 | Cisco IOS | Bus error at crypto_ikmp_config_authenticated |
| CSCse31818 | Cisco IOS | Traceback if_index_open_port_to_speak seen when ISSU with 12.2SG/SGA |
| CSCse37042 | Cisco IOS | BOOM: Adj are not getting resolved for the directly connected vrf en int |
| CSCse42370 | Cisco IOS | BOOM: STNDBY Rest , active crash while applying SP on SIP600 output int |
| CSCse48657 | Cisco IOS | config sync will reset standby when no EEM policy only on active |
| CSCse53517 | Cisco IOS | WiSM: Tracebacks seen after SSO switchover |
| CSCse57081 | Cisco IOS | NACL2IP: Clientless IP Phone triggers authentication to ACS every minute |
| CSCse63833 | Cisco IOS | SNMP bus error while polling cipsStaticCryptomapTable . |
| CSCse67736 | Cisco IOS | Add support for XFP-ZR optics |
| CSCse69570 | Cisco IOS | Leakage of VRF routes in global routing table |
| CSCse72688 | Cisco IOS | In sup720, ingress packet info. of GRE tunnel was not exported to server |
| CSCse78548 | Cisco IOS | LSR adds incorrect label stack (label 1) |
| CSCse82589 | Cisco IOS | LSR mishandles packets with router-alert label |
| CSCse89636 | Cisco IOS | LFD-3-INVINSTALLER LSD-3-LABEL msgs and tracebacks when PRE2 -PRE3 ISU |
| CSCsf08502 | Cisco IOS | event_reqinfo event_pub_sec/event_pub_msec missing for event_none events |
| CSCsf08803 | Cisco IOS | event snmp may wrongly triggered when using type increment |
| CSCsf22829 | Cisco IOS | EEM Interface event detector sets old value to the sample value |
| CSCsf27677 | Cisco IOS | crash on V122_31_SB_THROTTLE image with fix for CSCse89636 |
| CSCsf97859 | Cisco IOS | invalid shows in show hw-module subslot with SPA-OC192POS-LR |
| CSCsg01644 | Cisco IOS | EEM debug event manager tcl cli sent to the console, script may crash |
| CSCsg09654 | Cisco IOS | c7304:COMMON_FIB-2-HW_IF_INDEX_ILLEGAL |
| CSCsg13828 | Cisco IOS | fh_fd_timer.proc crashed without any special trigger |
| CSCsg14063 | Cisco IOS | SPA-[2/4]XOC48POS/RPR voltage reading needs parameter checking |
| CSCsg21809 | Cisco IOS | Add bridge asic status collection support . |
| CSCsg22830 | Cisco IOS | Standby not coming up after sso switchover |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg28331 | Cisco IOS | AB: SIP600: LC memory leak on PW VC switchover |
| CSCsg29305 | Cisco IOS | hw-module subslot reload crashes the router . |
| CSCsg41017 | Cisco IOS | VSA crashes on tunnel bring up with 1000IKE/1000GRE with pki |
| CSCsg47039 | Cisco IOS | SIP-600/ES20 LC crash following TE-FRR scenario on tunnel recovery |
| CSCsg57611 | Cisco IOS | PBHK id missing in IP and Interface session accounting start records . |
| CSCsg67551 | Cisco IOS | LDP session starts to flap after graceful-restart on switchover |
| CSCsg75132 | Cisco IOS | REDUNDANCY-3-IPC: cannot open standby port session in use |
| CSCsg86046 | Cisco IOS | Unable to monitor traffic in the clear when using the vrf vpn config |
| CSCsg86567 | Cisco IOS | MDT tunnel reuse at stby causing %IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP |
| CSCsg87235 | Cisco IOS | EEM config prevents telnet connection |
| CSCsg87747 | Cisco IOS | RECV_PVID_ERR message received with bringing up etherchannel trunk |
| CSCsg96495 | Cisco IOS | IF--Index: Allow recovery following hwidb->hw_if_index being set to -1 |
| CSCsg98045 | Cisco IOS | EEM track event detector missing maxrun option for tcl scripts |
| CSCsg98612 | Cisco IOS | Speed nonegotiate CLI option missing for SIP-600/ESM-20 eth ports |
| CSCsg99996 | Cisco IOS | on a ERP_CLIENT: Timer event IPC versioning process gets stuck |
| CSCsh17328 | Cisco IOS | WS-SVC-WISM-1-K9 reports 0.0 in entPhysicalVendorType |
| CSCsh17579 | Cisco IOS | Transceiver TX Power displays erroneous TX level |
| CSCsh17630 | Cisco IOS | HA: Standby reset with invalid config |
| CSCsh28014 | Cisco IOS | After unconfig MPLS, seen %SCHED-CFC8-3-UNEXPECTEDEVENT & Traceback |
| CSCsh30143 | Cisco IOS | COMMON_FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface if=0 |
| CSCsh30617 | Cisco IOS | EEM software forced crash when unregistering an applet |
| CSCsh34536 | Cisco IOS | CEOP: CEM group config lost on standby RP |
| CSCsh35451 | Cisco IOS | stbySP crash after LV-RV-RVSO-RV w/ MDR SM blockin RF in RF_PROG_ACTIVE |
| CSCsh42678 | Cisco IOS | C2W2:SWITCH_BUS_IDLE on standby SP after RV |
| CSCsh56121 | Cisco IOS | Losing RSA keys on Standby Supervisor after switchover or reload |
| CSCsh57238 | Cisco IOS | SXF6:sh int cmd on 6148 cards display zero o/p drops even with qos drops |
| CSCsh61002 | Cisco IOS | SPA-5X1GE: GE-port not transmitting after 'shut/no shut' and vica versa |
| CSCsh64820 | Cisco IOS | ISSU Abort imme after RunV cause act/stby with new/old image |
| CSCsh74385 | Cisco IOS | EEM fails to register with the redundancy framework (RF) |
| CSCsh74417 | Cisco IOS | crash in c10k_remote_crash_interrupt |
| CSCsh74962 | Cisco IOS | Interface Bounce holding CAC limit unable to accept IKE session. |
| CSCsh83272 | Cisco IOS | We need to have consistency-check type rp-sp by default |
| CSCsh83362 | Cisco IOS | Xconnect down as L2TPv2 to PPP-AC switching not enabled after reload |
| CSCsh84657 | Cisco IOS | STP Loopguard: Ability to disable loopguard for Po270 and higher for FWM |
| CSCsh96342 | Cisco IOS | PVID inconsistency handled incorrectly when running MST |
| CSCsh97395 | Cisco IOS | IDSM: Monitor config was removed after RPR switchover |
| CSCsh97848 | Cisco IOS | Sierra: LACP pdus should be untagged . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsi00377 | Cisco IOS | Exit Mismatch when application & prefix with common dst have diff policy |
| CSCsi05265 | Cisco IOS | SYS-2-GETBUF: Bad getbuffer -Process= LSDp Input Proc |
| CSCsi05515 | Cisco IOS | Entrance Load and Range on by default |
| CSCsi05566 | Cisco IOS | Configured ACL not formatted correctly when controlling applicaton |
| CSCsi09699 | Cisco IOS | OER -Inside prefixes not learned rom BGP for egress optimization |
| CSCsi22093 | Cisco IOS | Standby resets more than once, w red mode change + write mem |
| CSCsi28462 | Cisco IOS | Unable to initialize the SASL client on the peer router. |
| CSCsi31755 | Cisco IOS | BEEP IO handler hogs cpu and memory |
| CSCsi32646 | Cisco IOS | %UTIL-3-IDTREE_TRACE: PW freelist DB:Duplicate ID free for 14463433 |
| CSCsi43654 | Cisco IOS | SIP-600: EXCEEDGUAR msg appears when boot with interface bandwidth |
| CSCsi46510 | Cisco IOS | Gig port goes down on switchover, TB @ process_unlock_semaphore |
| CSCsi49150 | Cisco IOS | %PM-SP-4-PORT_BOUNCED: Port Gi9/3 was bounced by Consistency Check IDBS |
| CSCsi52382 | Cisco IOS | radius attribute 5 nas-port not sent in access-request for RA VPN users |
| CSCsi55428 | Cisco IOS | FRU Trap sequence incorrect when " hw-module subslot shutdown unpowered" |
| CSCsi58211 | Cisco IOS | Link flap under load with XENPAK-10GB-LW |
| CSCsi63649 | Cisco IOS | %SYS-3-TIMERNEG:Cannot start timer with negative offset,TTY Background |
| CSCsi70224 | Cisco IOS | NRT: STANDBY BOOT VAR disappears after HA switchover |
| CSCsi80642 | Cisco IOS | EzVPN ISAKMP rekey fails due to invalid proposal |
| CSCsi82166 | Cisco IOS | BEEP Router crashes at user_pw_lookup with 12.4(13.13)T1 image |
| CSCsi84417 | Cisco IOS | router hang/crash and cpuhog msgs seen when attaching service-policy |
| CSCsi85453 | Cisco IOS | cfg-sync failed  if switchport config is pasted on active & stby restart |
| CSCsi85532 | Cisco IOS | c851 crash w/o specifying pw-class in pseudowire |
| CSCsi92079 | Cisco IOS | OER system disabled fatal error . . |
| CSCsi94738 | Cisco IOS | 8xCHT1/E1 SPA modules not in entAliasMappingIdentifier |
| CSCsi96685 | Cisco IOS | Crash in chunk free called by sss_free_switch |
| CSCsi97434 | Cisco IOS | A router may crash when ipsec is established |
| CSCsi99875 | Cisco IOS | BOOM: spa_eeprom_read_bit on BOOTUP |
| CSCsj00870 | Cisco IOS | CAT6000: ICC client shall use ipc_return_message under error conditions |
| CSCsj01961 | Cisco IOS | ifindex table size from nvram sould be validated before malloc |
| CSCsj03212 | Cisco IOS | blade get into bad b2b state if it is not b2b ready |
| CSCsj04201 | Cisco IOS | %MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC: RP failed allocating IPC buffer |
| CSCsj06641 | Cisco IOS | LI: Traceback found in creating entry in cTap2StreamTable |
| CSCsj08713 | Cisco IOS | Disable bfd on SVI interfaces |
| CSCsj12034 | Cisco IOS | fabric switching-mode allow dcef-only- config makes stby stuck at rommon |
| CSCsj14565 | Cisco IOS | ACL = deny; sa request ignored when crypto local-address is dynamic |
| CSCsj19316 | Cisco IOS | Standby resets while booting up due to  %FILESYS-4-RCSF error |
| CSCsj20130 | Cisco IOS | %QM-2-TCAM_ERROR: TCAM programming error 20 |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj21464 | Cisco IOS | EPM dACL enhancements and EPM SSO support |
| CSCsj25470 | Cisco IOS | EEM hostnames over 20 characters causes CLI actions to hang |
| CSCsj27436 | Cisco IOS | c7600 duplicate and INVALID mls mpls label entries in FIB |
| CSCsj32493 | Cisco IOS | IPSEC: Incorrect IPSec connection info in InvalidSPI testing |
| CSCsj36327 | Cisco IOS | SPA-4XOC48POS/RPR won't come up after reload |
| CSCsj37398 | Cisco IOS | Properly initialize the Tycho register AC_QOS_DEFAULT_EGRESS (0x334) |
| CSCsj38796 | Cisco IOS | LC/SP crash @ label_entry_get_inlabel |
| CSCsj40695 | Cisco IOS | EEM: Incorrect TCL event registration string can hang or crash device |
| CSCsj42098 | Cisco IOS | SupV drops big packets destinated to a GRE Tunnel when frag. needed . |
| CSCsj43677 | Cisco IOS | Active Sup720 crash when removing Standy supervisor |
| CSCsj43962 | Cisco IOS | ISG interface responds to ARP for GLBP VIP with own MAC |
| CSCsj48453 | Cisco IOS | AW: CAT6k does not forward multicast traffic to WISM in L3 mode |
| CSCsj49293 | Cisco IOS | POS Interface  Output Rate (200 mbps) > Line rate (155 Mbps) |
| CSCsj53663 | Cisco IOS | EEM: RP crashed at fh_fd_syslog_event_match |
| CSCsj57351 | Cisco IOS | SU07 ME-C3750 crashed during elmi test |
| CSCsj58287 | Cisco IOS | 7600-SSC-400 crashes on reload |
| CSCsj58538 | Cisco IOS | Lots of prowler/patriot interface go down for few second during sso swov |
| CSCsj59997 | Cisco IOS | VTI tunnel: Arp for tunnel destination instead next hop. |
| CSCsj60006 | Cisco IOS | QoS: 'match ip rtp 65530 5' though accepted is not showing up in sh run |
| CSCsj60182 | Cisco IOS | IPSEC Tunnels not coming up in transport adjency mode |
| CSCsj65189 | Cisco IOS | Traffic stops over EOM ckt after SSO and followed by TE FRR cutover |
| CSCsj65755 | Cisco IOS | Packet loss with SPI NOT Available message during rekey . |
| CSCsj70303 | Cisco IOS | BOOM :Alignment error found @ ha_send_cfg_change_internal. |
| CSCsj74617 | Cisco IOS | MFI static-label configuration does not sync to slave RP |
| CSCsj77885 | Cisco IOS | %HA_EM-7-FMS_POLICY_MAX_ENTRIES message because of teminal length limit |
| CSCsj78751 | Cisco IOS | ES20: shut & no shut on ZR XFP causes the port to stay down |
| CSCsj78820 | Cisco IOS | MEM leak in Crypto IKMP process(crypto_ikmp_author_get_attributes) |
| CSCsj80655 | Cisco IOS | timer value overflows when the specified val is larger than a long val |
| CSCsj85897 | Cisco IOS | SPA-TE1-Linkrec's out of sync between SPA and LC |
| CSCsj86153 | Cisco IOS | Modular IOS CPU load oscillates even under constant load |
| CSCsj87687 | Cisco IOS | Crash during startup with  mpls configured |
| CSCsj89905 | Cisco IOS | EEM applet hangs if system prompt is changed |
| CSCsj90252 | Cisco IOS | SYS-3-CPUHOG IP RIB Update seen on Active RP |
| CSCsj90758 | Cisco IOS | UUT with BGP/DMVPN crashes after restarting iprouting.iosproc |
| CSCsj91961 | Cisco IOS | Ifnums of channels for E3 dont match on active and stdby |
| CSCsj94539 | Cisco IOS | Spurious Alarms in PA-MC-8TE1+ may cause router crash |
| CSCsj98198 | Cisco IOS | When we have only 1 flow in TT, flows are not exported to MC |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj98492 | Cisco IOS | Pak subblock handlers need to be part of packet library |
| CSCsk02456 | Cisco IOS | TBs found @ pm_assert_fail. . |
| CSCsk04241 | Cisco IOS | XFP occasionally goes into module not-ready state after enabling laser |
| CSCsk07255 | Cisco IOS | Sip-600 crash on SSO |
| CSCsk08329 | Cisco IOS | inbound service-policy traffic incorrectly seen in default-class |
| CSCsk16240 | Cisco IOS | C2W1: active not responding msgs seen om reload with 41patches |
| CSCsk16706 | Cisco IOS | AB76:Unable to configure cwan int in SSO- standby doesnt support cmd |
| CSCsk17449 | Cisco IOS | GLBP debug is shown for non-GLBP addresses |
| CSCsk19817 | Cisco IOS | shut/no shut causes pm failed get pm mp semaphore |
| CSCsk19866 | Cisco IOS | Unable to boot boomerang image on sup720 |
| CSCsk21354 | Cisco IOS | PAT : Missing second Netflow shortcut after route change. |
| CSCsk26456 | Cisco IOS | SPA-4XOC3-ATM does not pass traffic after SPI4 source FIFO overflow err |
| CSCsk27081 | Cisco IOS | ifHCInOctets and ifHCOutOctets on GE-WAN interfaces wrap up at 2^32 |
| CSCsk32872 | Cisco IOS | Wrong API usage, can lead to crash . |
| CSCsk33045 | Cisco IOS | MST BPDU *must* be sent untagged, even when the switch is configured wit |
| CSCsk37675 | Cisco IOS | IKE stuck after several hours of IKE SA rekey . |
| CSCsk38937 | Cisco IOS | Loss of traffic for more than 15 seconds when PRE2 failover to standby |
| CSCsk39340 | Cisco IOS | IPRM process runs at 100% CPU for more than 30 mts |
| CSCsk40931 | Cisco IOS | Port Security Inactivity Aging is not working as expected |
| CSCsk41134 | Cisco IOS | ISAKMP SA neg not successful for in tunnel mode w/ RSA-SIG |
| CSCsk44233 | Cisco IOS | While raising the interrupt level, bgp_route_map_inform tries to suspend |
| CSCsk45585 | Cisco IOS | Heathland: On bootup MPLS not supported on platform message |
| CSCsk48089 | Cisco IOS | Enhance  "ip policy route-map" command for backward compatibility |
| CSCsk49151 | Cisco IOS | Vlan policy-map rejected upon reloading. |
| CSCsk58040 | Cisco IOS | WS-X6148A-GE-45AF retains previous modules MACs after OIR |
| CSCsk60112 | Cisco IOS | NRT:NSE-150 is not initializing the memory to zero before assign a value |
| CSCsk60912 | Cisco IOS | MPLS forwarding table empty on standby RP . |
| CSCsk63657 | Cisco IOS | Not able to sync up to loopback line on SPA-1XOC12-POS |
| CSCsk64543 | Cisco IOS | PoE Power Calculations Incorrect |
| CSCsk64625 | Cisco IOS | VPLS pkt drops in xchip when TE tunnel path changes to alternate path |
| CSCsk67417 | Cisco IOS | Crash while two or more users displays: show ip arp inspection log |
| CSCsk67457 | Cisco IOS | BCP-MLP:Traffic stops flowing making one link shut on multilink |
| CSCsk67578 | Cisco IOS | Flow End sysUpTime higher value than the Router sysUpTime |
| CSCsk70628 | Cisco IOS | MST : Not subtracting remaining hop count of agreement BPDU |
| CSCsk73627 | Cisco IOS | WS-X6548-GE-TX powered down due to keep alive polling feature |
| CSCsk73838 | Cisco IOS | After fabric tiemout is seen, line card did not recover using earl patch |
| CSCsk77282 | Cisco IOS | EEM RPC file descriptor leak |

| Identifier | Technology | Description |
|---|---|---|
| CSCsk77462 | Cisco IOS | IETF Class attribute is missing in radius accounting record |
| CSCsk77648 | Cisco IOS | HA: issu image-version compatibility en/dis not function properly. |
| CSCsk78390 | Cisco IOS | Naxos crashes while trying to fpd upgrade granikos |
| CSCsk80552 | Cisco IOS | Shut and no shut of interface causes the delay in forming rp mapping |
| CSCsk82191 | Cisco IOS | Multicast groups sometimes not populated on switchover. |
| CSCsk82370 | Cisco IOS | RP crash and tracebacks in crypto related process |
| CSCsk83089 | Cisco IOS | Increase maximum aggregate policer > 10Gbps |
| CSCsk83683 | Cisco IOS | VRF-Lite aware PBR feature does not work after reload/SSO swover |
| CSCsk83954 | Cisco IOS | Traceback on wan linecards on bootup if mpls access-list configured |
| CSCsk84443 | Cisco IOS | cempMemPoolEntry return worng value |
| CSCsk84498 | Cisco IOS | EVERGLADES:archive,write-mem feature broken |
| CSCsk86114 | Cisco IOS | SRB2:spa-atm: SIP200 crashes at checkheaps_process on atm shut noshut . |
| CSCsk86381 | Cisco IOS | KMI memory leak in 'IPSEC key engine' when delete p2 failed |
| CSCsk86510 | Cisco IOS | DSCP in outer IP copied from MPLS EXP on MPLS->GRE path |
| CSCsk88273 | Cisco IOS | Traceback seen @edisms on clearing counter on Active SP |
| CSCsk89091 | Cisco IOS | HWIF-QOS-ERR: Failure installing Port QoS TX/Rx setting |
| CSCsk89852 | Cisco IOS | VS2: MEC (LACP) members flap when native subinterface is configured |
| CSCsk89970 | Cisco IOS | SPA-IPsec-2G: Don't add Vlan 1 to Wmac & HMAC trunk interface by default |
| CSCsk93354 | Cisco IOS | High CPU on stby PRE due to BEM VERIFY . |
| CSCsk93366 | Cisco IOS | lte_rp_get_lte_update_xdr_size/fib_upd_consume_rec_meets_upd_rec crash |
| CSCsk94870 | Cisco IOS | VS2: TB @ ether_extract_addr |
| CSCsk97144 | Cisco IOS | wait for remote process DiagCard7/-1creation times out with 1018 ION |
| CSCsl02190 | Cisco IOS | ICMPv6 to all node multicast address fail . |
| CSCsl04500 | Cisco IOS | OBFL process causing 6708 high CPU |
| CSCsl05874 | Cisco IOS | MPLS-MFI: mpls fragmentation not working in particle-based routers |
| CSCsl06059 | Cisco IOS | Router crash at route_map_vrf_af_change_nh |
| CSCsl06577 | Cisco IOS | Linking bootflash to bootdisk failed after pcmcia_driver.proc restart |
| CSCsl07575 | Cisco IOS | If VC comes up after policy is applied, VC traffic goes to class-default |
| CSCsl08596 | Cisco IOS | C2W1B: portType and entPhysicalVendorType of 10GBase-LRM is incorrect |
| CSCsl08912 | Cisco IOS | Vlan access list not working when have "xconnect vfi #" under the SVI |
| CSCsl10489 | Cisco IOS | OER ignores MOS score of jitter probe when INPOLICY timer expires |
| CSCsl11335 | Cisco IOS | MVPN-MIB:Entries obtained from "ciscoMvpnBgpMdtUpdateTable" is incorrect |
| CSCsl11868 | Cisco IOS | With IP CEF enabled ACL is not denying packets as intended. . |
| CSCsl12121 | Cisco IOS | Sierra: TB(Spurious memory access) when get ciscoPortSecurityMIB |
| CSCsl12827 | Cisco IOS | Handling Transit IpSec in VRF mode |
| CSCsl12836 | Cisco IOS | CPUHOG in OBFL VOLT bootflash process |
| CSCsl13477 | Cisco IOS | SSO not working with crypto maps terminating at same peer address . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl16353 | Cisco IOS | Problem in SIP400 Vpls Frr Link Protection |
| CSCsl17798 | Cisco IOS | Etherchannel state inconsistent between active and standby |
| CSCsl18525 | Cisco IOS | Standby-SP doesn't have mfib table |
| CSCsl18765 | Cisco IOS | 6500-7600 : SPAN of EoMPLS port causes packet reflection or loop |
| CSCsl18918 | Cisco IOS | 12.2SRA: Disable Cell Packing . |
| CSCsl19708 | Cisco IOS | Naxos : Disable Telesto Internal TERMINATION For Reference Clock, PB RAM |
| CSCsl20701 | Cisco IOS | EEM RPC memory leak in fh_fd_rpc_get_filename and ifs_simple_open_common |
| CSCsl21171 | Cisco IOS | Crypto syslog messages span multiple packets |
| CSCsl26033 | Cisco IOS | Modifying the BFG doesn't re-create the SA's |
| CSCsl26998 | Cisco IOS | Switch crashes on applying PBR with next-hop verify-availability |
| CSCsl27236 | Cisco IOS | %SYS-3-CPUHOG: Task is running for (126000)msecs, causes RP crash . |
| CSCsl27957 | Cisco IOS | %EC-SP-5-CANNOT_BUNDLE2 is seen after inserting WS-SVC-FWM-1 |
| CSCsl28371 | Cisco IOS | SPA-IPsec-2G VRF: L2 loop and broadcast storm may occur on default vlans |
| CSCsl30308 | Cisco IOS | PIM snooping corrupts PIM RPF Proxy packet |
| CSCsl32940 | Cisco IOS | Router crashes while reloading Naxos |
| CSCsl34481 | Cisco IOS | IPV6-MCAST:router crashes while unconfiguring ipv6 mcast routing |
| CSCsl34515 | Cisco IOS | VS2:after SSO with preemption, port security is broken |
| CSCsl34612 | Cisco IOS | RP faced a Modular IOS kernel crash in mem_vmem_free |
| CSCsl34717 | Cisco IOS | TMS_PI1:Syslog missing consumer device-id |
| CSCsl35325 | Cisco IOS | MRIB client remains after a linecard removal |
| CSCsl39691 | Cisco IOS | Config Sync:Bulk-sync failure due to Servicing Incompatibility after SSO |
| CSCsl40528 | Cisco IOS | VS2: Port-channel fails to forward unicast packets after switchover . |
| CSCsl41230 | Cisco IOS | IPSec SPA breaks IPSec if interesting traffic uses TCP ports |
| CSCsl43540 | Cisco IOS | VS2:snmp mac notification for port channel on DFC linecard doesn't work |
| CSCsl51380 | Cisco IOS | Sup720 and Sup32 TCAM & SSRAM Consistency Checkers refinement |
| CSCsl51395 | Cisco IOS | slot_earl_icc_shim_addr:device crash with hw-module reset |
| CSCsl52092 | Cisco IOS | DHCP db agent considers port-channel interface (poX) as invalid |
| CSCsl53037 | Cisco IOS | Mail action does not separate headers from body |
| CSCsl53279 | Cisco IOS | Physical interfaces on Cat6k set to 10 usec regardless of line speed |
| CSCsl53727 | Cisco IOS | Add UDLD interface counters for debugging purpose |
| CSCsl53845 | Cisco IOS | sup720/SXH: dummy packet send over inband when sw netflow is used |
| CSCsl54630 | Cisco IOS | Memory leak after create-apply-remove-delete policies on QM Process RP |
| CSCsl57993 | Cisco IOS | Everglades: MC crash on executing 'sh oer mas traffic-class learned' |
| CSCsl58673 | Cisco IOS | EEM Prevents VTY telnet to MCP router |
| CSCsl58924 | Cisco IOS | Standby SP crashed due to TestAclDeny failure on bootup/switchover |
| CSCsl59553 | Cisco IOS | SIP-400: bursty traffic causes packet drop even in low rates |
| CSCsl61164 | Cisco IOS | Router may crash @ipflow_fill_data_in_flowset when changing flow version |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl62341 | Cisco IOS | ip rip summary address cannot be applied to VAI |
| CSCsl62344 | Cisco IOS | Call-home:parser error and profiles are deleted after reload |
| CSCsl63311 | Cisco IOS | 6500 May Experience High CPU due to NAT traffic |
| CSCsl69123 | Cisco IOS | SIP-400:QoS:Police drops MPLSCP, CDPCP negotiation packets - SRA,SRB |
| CSCsl70016 | Cisco IOS | WS-X6516A-GBIC card in switch 2 goes down frequently in vsl |
| CSCsl70148 | Cisco IOS | PIM enabled p2p Crypto GRE Tunnels not installed in Hardware |
| CSCsl70408 | Cisco IOS | Standby PRE fails to reach SSO due to BEM CPU hog |
| CSCsl70667 | Cisco IOS | 12.2(33)SRB2: LC crash at fib_fib_feature_space_xdr_decode |
| CSCsl71704 | Cisco IOS | VS2:RACL not applied  on MEC after disabling netflow & chng flowmask |
| CSCsl72332 | Cisco IOS | cat6k crash with 'no mobility network-id 4' |
| CSCsl72752 | Cisco IOS | VS2: after preempted switchover, interface states are out of sync |
| CSCsl72826 | Cisco IOS | Router Crash @ ipfib_policy_forward |
| CSCsl72912 | Cisco IOS | VS2: WS-X6708 DFC crash in local_cb1(Segment violation) |
| CSCsl74456 | Cisco IOS | VPN-SPA : TCAM not programmed on POS sub-interface after a reload |
| CSCsl74976 | Cisco IOS | Punted MPLS-tagged traffic causes control plane instabilities |
| CSCsl75136 | Cisco IOS | Cat6k with Sup32 failed to boot up after power cycle. |
| CSCsl75164 | Cisco IOS | Router crash when 'clear cry session' |
| CSCsl75719 | Cisco IOS | sxf13 show int tunnel with blank display |
| CSCsl75836 | Cisco IOS | VS2: MCAST LTL T/B's observed, when removing VLAN / SVI used for mcast |
| CSCsl76647 | Cisco IOS | VPN SPA Cannot clear SA using conn-id with CLI |
| CSCsl78582 | Cisco IOS | 12.2SRC:SSO :%COMMON_FIB-3-FIB_PATH_LIST_DB:Attempt to add empty path |
| CSCsl79141 | Cisco IOS | Vlan mode EoMPLS new VC does not come up after SIP-600 reload |
| CSCsl79195 | Cisco IOS | XDR issu negotiation failed for standby SP after switchover |
| CSCsl79219 | Cisco IOS | mvpn : bidir shadow entries not installed |
| CSCsl79781 | Cisco IOS | EEM config causes config-sync PRC mismatch error with "do" command |
| CSCsl80682 | Cisco IOS | SPA crashes if crypto acl changed |
| CSCsl83211 | Cisco IOS | Sup32 running ION image fails to bootup after a power-cycle. |
| CSCsl83212 | Cisco IOS | Traceback logs are seen when deleting auto-template interface |
| CSCsl84317 | Cisco IOS | Active crashes on applying acl to EoMPLS subif on SIP-600 |
| CSCsl87677 | Cisco IOS | changing the access vlan doesn't reflect the vlan of the secure configur |
| CSCsl87843 | Cisco IOS | GLBP: AVF flaps on changing to lower interface address |
| CSCsl89069 | Cisco IOS | Zamboni crashed at illegal event/state combinationin CfgMonInd, clear sa |
| CSCsl89176 | Cisco IOS | Cat6k may crash when vlanTrunkPortEntry is polled via snmp |
| CSCsl89425 | Cisco IOS | BFD sessions dont scale |
| CSCsl89890 | Cisco IOS | VS2: crash in psecure-process_timer |
| CSCsl91085 | Cisco IOS | system/iprouting.iosproc crash after activate 39 dummy/restart patches |
| CSCsl92286 | Cisco IOS | 60 second multicast traffic loss as VSS standby chassis initializes |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl92475 | Cisco IOS | CAM entries not removed after EtherChannel down |
| CSCsl93559 | Cisco IOS | Unsupported ISL encap CLI option should be disabled on 6716 |
| CSCsl94301 | Cisco IOS | VS2: Mac learning in linecard gets disabled by pre-emption switchover. |
| CSCsl98238 | Cisco IOS | QoS statistics-export only exports to directly-connected destinations |
| CSCsm01399 | Cisco IOS | Bus idle recovery may cause 10GE interface to remain down |
| CSCsm04256 | Cisco IOS | CPUHOG and crash after 'show memory detailed all statistics' issued |
| CSCsm04824 | Cisco IOS | OER Top Talker Functionality broken on s3223 |
| CSCsm05486 | Cisco IOS | mtu mis probram in adj thru tunnel interface after b2b failover |
| CSCsm08087 | Cisco IOS | Arp unresolved after sh/nosh of egress int ;route-map applied at ingress |
| CSCsm08830 | Cisco IOS | Config-Sync: BadCode fix for CSCed88426 |
| CSCsm08971 | Cisco IOS | SEA:Soft reload occurs everytime after issue show cmd's and T/B with mz |
| CSCsm11717 | Cisco IOS | VS2:On reloading standby chassis T/Bs on SP console for 1 minute |
| CSCsm11898 | Cisco IOS | IOS:SLB: Incorrect NAT Translation when Nat client is enabled |
| CSCsm12692 | Cisco IOS | 6VPE:RP switchover need for about 10 minutes to resume IPv6 traffic |
| CSCsm13389 | Cisco IOS | RRI is not called be if QM rekey timer expiry forces SA deletion |
| CSCsm14915 | Cisco IOS | Stack overwrite crash with large No of GLBP IPv6 groups on interface |
| CSCsm15350 | Cisco IOS | vpnspa crashed at assert failure in l2-mcpu.c on line |
| CSCsm15687 | Cisco IOS | SIP-600 GE subints fail with crypto connect & VPN SPA |
| CSCsm16309 | Cisco IOS | Fastpath thread crash in BFD code after all BFD sessions went down |
| CSCsm17066 | Cisco IOS | GLBP forwarders flap on SSO |
| CSCsm17983 | Cisco IOS | Memory corruption by  l3_mgr_e7_fmask_init_platform |
| CSCsm19550 | Cisco IOS | sup720 rx intr should check tx descriptor exhaustion |
| CSCsm20994 | Cisco IOS | kron job daily reoccurences fail after new year |
| CSCsm21126 | Cisco IOS | C7600-SSC-400: Resync fabric interface on fabric error |
| CSCsm22385 | Cisco IOS | V4 VPN traffic stops after toggling agg. label between vpn-cam and tcam |
| CSCsm23160 | Cisco IOS | RFS: rf task attempted to unlock semaphore owned by interrupt |
| CSCsm24904 | Cisco IOS | Bridge-mib timing out dot1dBasePortIfIndex |
| CSCsm24906 | Cisco IOS | IPV6 neighbour discovery not working on SVI intf under VRF |
| CSCsm25061 | Cisco IOS | ike fragments dropped by vpnspa |
| CSCsm26063 | Cisco IOS | C2W2:Active RP Crash on sh/no sh of intf with ipv6 address configured |
| CSCsm26415 | Cisco IOS | Traceback seen when show platform cfm issued for fwd_vlan 0 |
| CSCsm27017 | Cisco IOS | VS2: power configuration is not synced to standby |
| CSCsm28287 | Cisco IOS | Active RP crash on shutdown of GRE tunnel followed by switchover |
| CSCsm30584 | Cisco IOS | cwpa2 card crashes after attaching and removing service policy |
| CSCsm30858 | Cisco IOS | PIM register packets upmarked to TOS 6 by PTcam redirection |
| CSCsm31178 | Cisco IOS | policy-map stops working on a good int if wrongly applied on another int |
| CSCsm32363 | Cisco IOS | Netflow SLB sw-installed entries not aging out |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm32493 | Cisco IOS | Backout of CSCsh94882 |
| CSCsm33528 | Cisco IOS | Rekey packet loss for pure ipsec |
| CSCsm35364 | Cisco IOS | SPA-IPSEC-2G get reload automatically by RP |
| CSCsm37673 | Cisco IOS | Traffic from SSLM service module not going over multi-module etherchanne |
| CSCsm38962 | Cisco IOS | LLDP Port-ID and Port-Description TLVs are interchanged |
| CSCsm40606 | Cisco IOS | WS-X6724 SFP get's reboots again and again with TestSynchedFab Failed |
| CSCsm43962 | Cisco IOS | Cat6k L2TP packet looped through blocked port |
| CSCsm44309 | Cisco IOS | L2 Po - new member was not included in mapped ucast flood &mcast indices |
| CSCsm44413 | Cisco IOS | RP not added into LTL index when bridge-group is configured |
| CSCsm46017 | Cisco IOS | Process switching of ISL frame is not correct in sierra dueto CSCsl63311 |
| CSCsm46607 | Cisco IOS | dot1q subinterface and mac-address limits on same vlan cause stadby relo |
| CSCsm48287 | Cisco IOS | Drop counters for VPLS VC not incrementing |
| CSCsm48357 | Cisco IOS | crash at line by line config sync failure while unconfig FR xconnect |
| CSCsm49103 | Cisco IOS | I/O Memory Leak when running show mls cef command |
| CSCsm49440 | Cisco IOS | RRI: Need to support remote-peer option when source proxy == peer |
| CSCsm50309 | Cisco IOS | Crash due to ipflow aggregation when configuring OER in border router |
| CSCsm51299 | Cisco IOS | Code divergence caused a need for a second fix for CSCsl27236. |
| CSCsm54873 | Cisco IOS | EEM some time are not triggered properly |
| CSCsm56279 | Cisco IOS | C2W2: Important enhancements to "test swi vir ltl index" CLI |
| CSCsm56293 | Cisco IOS | Sup4:DFC only mode, create bus stall condition-the switch still crash |
| CSCsm59384 | Cisco IOS | DPD not deleting IKE SA's |
| CSCsm59488 | Cisco IOS | Fix backwards compatibility for multicast egress netflow cli |
| CSCsm59926 | Cisco IOS | RP receives 2 copies of each PIM register with MVPN |
| CSCsm59949 | Cisco IOS | vtp3:with 4k vlan HA reload/sso causes the standby to reload continuosly |
| CSCsm62179 | Cisco IOS | C2W2: MPLS pseudowire ping for SVI mode EoMPLSoGRE fails |
| CSCsm64424 | Cisco IOS | C2W1: Copy command generates spurious authorization requests |
| CSCsm66023 | Cisco IOS | IPv6 VTI RP crashed ace_reverse_map when changing tnlsrc from v4 to v6 |
| CSCsm66280 | Cisco IOS | TIDP: Router crashes at tidp_find_or_add_peer |
| CSCsm66602 | Cisco IOS | SIP 400 loses VPLS VC entry on shutting down the MPLS TE tunnel |
| CSCsm66678 | Cisco IOS | Policing not working in MPLS cloud |
| CSCsm69112 | Cisco IOS | Multicast output drop w/ IGMP snooping @ near line rate 1Gbps |
| CSCsm69827 | Cisco IOS | %SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3 |
| CSCsm70349 | Cisco IOS | BPDU traffic over Eompls is not switched on 3C system |
| CSCsm70707 | Cisco IOS | WS-X6748-SFP shutdown(Could not set appropriate Switching mode) |
| CSCsm70774 | Cisco IOS | Router crashes at cfg_kron_plcy_sbmd_cmd. |
| CSCsm71537 | Cisco IOS | divide by 0 crash in oer_br_update_iface_counters |
| CSCsm72807 | Cisco IOS | DHCP packets can get corrupted in an SSO environment |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm73395 | Cisco IOS | Per-User ACL install error |
| CSCsm73592 | Cisco IOS | Crash when removing tunnel interface. |
| CSCsm75020 | Cisco IOS | EARL7 Additional ECC Error Handling enhancements |
| CSCsm75286 | Cisco IOS | bgp route-map doesn't work correctly when deleted part of sequences |
| CSCsm76172 | Cisco IOS | Memory held by "mls-hal-agent" process in standby-sp |
| CSCsm77171 | Cisco IOS | Router crash when "ip flow" enabled. |
| CSCsm79344 | Cisco IOS | Bogus "TCAM MASK entry capacity exceeded" message |
| CSCsm81399 | Cisco IOS | No Such Instance error from many SNMP objs for 1xOC48 POS/RPR SPA |
| CSCsm82169 | Cisco IOS | VSS: heathland interfaces are err-disabled on standby chassis |
| CSCsm82264 | Cisco IOS | VS2: Entire VSS system goes down after restarting call-home process |
| CSCsm82382 | Cisco IOS | 7600 standby RP memory leaking cause CEF disable |
| CSCsm82472 | Cisco IOS | DAI: L2-Portchannel formed for member's DAI trust mismatch |
| CSCsm82958 | Cisco IOS | radius sticky entry deleted even if the idle timer is not 0 |
| CSCsm83893 | Cisco IOS | W2: "sh mls cef adj mpls detai"l after SSO freeze RP causeT/B , reboot |
| CSCsm83948 | Cisco IOS | CISCO7609 returns sysObjectId as ciscoProducts.402 (which is cisco7606) |
| CSCsm84257 | Cisco IOS | crash in ipflow_periodic context due to watchdog timeout |
| CSCsm84267 | Cisco IOS | Tracebacks & %CPU_MONITOR-SP-6-NOT_HEARD: messages with NAT. |
| CSCsm85936 | Cisco IOS | UUT cpu at 40% with bi-dir traffic across a single tunnel |
| CSCsm86027 | Cisco IOS | B2B failover,ace_tunnel_compare:Invalid address_type, router crashed |
| CSCsm92183 | Cisco IOS | c2w1: Heathland card is not coming up due to diag failure |
| CSCsm92365 | Cisco IOS | c76 router loses its vlan database after configuring VTPv3 |
| CSCsm93047 | Cisco IOS | IPSec uses incorrect SA lifetime during rekey |
| CSCsm93648 | Cisco IOS | C2W2:080226 Rtr crashed when moving tunnels from VTI to GRE/TP |
| CSCsm94421 | Cisco IOS | Configuring STP cost in an etherchannel to the defaulthas no effect |
| CSCsm95456 | Cisco IOS | Duplicate L3 packets with 6708 and DEC |
| CSCsm96243 | Cisco IOS | Switch crashes on executing sh tcam interface acl with include option |
| CSCsm96610 | Cisco IOS | OOB-MAC-SYNC is on, need to change internally the cam aging to 480 Sec |
| CSCsm97669 | Cisco IOS | Cat6K with NAT-T through PAT: IKE packets with src_port != 4500 dropped |
| CSCsm97836 | Cisco IOS | Memory leak VSL Manager |
| CSCsm98000 | Cisco IOS | ISSU upgrade procedure takes switch into RPR instead of SSO |
| CSCsm98256 | Cisco IOS | Berytos got power down due to TestMacNotification and TestFabricCh0Healt |
| CSCsm98671 | Cisco IOS | TestTrafficStress fails with certain configuration |
| CSCsm99079 | Cisco IOS | kron causes CPU HOG |
| CSCsm99690 | Cisco IOS | Netflow: Crash with aggregation caches and export to MPLS VPN |
| CSCso00104 | Cisco IOS | Router crashes on aggregation-type prefix-length and ACL changes to OER |
| CSCso00793 | Cisco IOS | ITP-76: Flexwan Memory version "VI4DP647228EBK-MD" causes reload |
| CSCso00864 | Cisco IOS | Standby sup crashed on configuing local-address command for cry map |

| Identifier | Technology | Description |
|---|---|---|
| CSCso02208 | Cisco IOS | VS2: crash when provisioning LI stream |
| CSCso03419 | Cisco IOS | VRF_Lite aware PBR: Set ip vrf clause changes on Reload/SSO with SIERRA. |
| CSCso05127 | Cisco IOS | WS-X6708-10GE crashes following upgrade to 12.2(33)SXH1 and 12.2(33)SXH2 |
| CSCso05889 | Cisco IOS | Pak Subblock creation fails from CEF in ION |
| CSCso05920 | Cisco IOS | cpmCPUMemoryFree incorrect for Posix memory |
| CSCso11489 | Cisco IOS | %SYS-SP-3-INVMEMINT while collecting ION crashinfo |
| CSCso11822 | Cisco IOS | LACP PC switchport, on OIR, "channel group 112 active" config gets lost |
| CSCso12405 | Cisco IOS | ViF multicast packets are process switched. IO mem  middle buffer leak |
| CSCso12903 | Cisco IOS | RE MET address check missing while running MET patch on IO bus timeout |
| CSCso13950 | Cisco IOS | implementation of cmasModuleActionNotif  in CSICO-MODULE-AUTO-SHUTDOWN-M |
| CSCso16532 | Cisco IOS | Entries missing from cam table with sh mac- multicast igmp-snooping cmd |
| CSCso18683 | Cisco IOS | IP DSCP Re-circulation not working as expected after issu runversion. |
| CSCso20519 | Cisco IOS | Cheronia: Fix SMB drive strength programming. |
| CSCso22987 | Cisco IOS | PBR requirement not met even if BRs are one-hop away through another BR. |
| CSCso28275 | Cisco IOS | Traffic polarization within a MEC on VSS. |
| CSCso28295 | Cisco IOS | MVPN Tunnel-sourced non-rpf traffic constantly dropped in software |
| CSCso28791 | Cisco IOS | MAC_MOVE-SP-4-NOTIF seen for L2TP packets over dot1q tunnel |
| CSCso29226 | Cisco IOS | IP source guard is not supported on ether channel member |
| CSCso30038 | Cisco IOS | A OIL is not registerd properly in mroute table with static igmp group |
| CSCso30598 | Cisco IOS | GLBP - SSO : Stby reload continuously after switchover on c7304 |
| CSCso30649 | Cisco IOS | vtp3:pvlans are not updated correctly on converting from off to server |
| CSCso31506 | Cisco IOS | IPv6 AH Extension Headers Punted to Software on PFC-3B & 3C |
| CSCso32193 | Cisco IOS | IPv6 software switched in Egress replication mode |
| CSCso37640 | Cisco IOS | DHCP snooping ACL's are not getting programmed after switchover. |
| CSCso38151 | Cisco IOS | Error/Traceback after power fail. %SPA-3-SW_ERROR: spa_get_card_info: |
| CSCso38671 | Cisco IOS | VS specific message seen on Sup32 image when "erase startup-config" |
| CSCso39444 | Cisco IOS | The new Active supervisor will crash after SSO @ fib_path_list_lock_memo |
| CSCso39518 | Cisco IOS | fh_policy_dir.proc process crash when activate 0E patch |
| CSCso39818 | Cisco IOS | Ingress Marking not working on SIP-600 on linecard reset/ toggle mlsqos |
| CSCso40891 | Cisco IOS | Stb rp reloaded during every bootup, process = FM, fm_free_platform_data |
| CSCso43539 | Cisco IOS | power converter failure reported before power was on |
| CSCso44072 | Cisco IOS | High CPU due to multicast traffic getting punted to software |
| CSCso45104 | Cisco IOS | PfR: Incoming Optimization BGP not working for connected routes on BR |
| CSCso46210 | Cisco IOS | VS: NAM on Standby switch not able to configure SPAN session |
| CSCso46337 | Cisco IOS | %MFI-SP-3-MFICOMM: un-matched frr_cutover_cnt after SSO switchover |
| CSCso49344 | Cisco IOS | Egress policing policy not programmed in SIP-600 after system reload. |
| CSCso50175 | Cisco IOS | % ENT_API-4-NOPORT: Traceback seen after switchover |

| Identifier | Technology | Description |
|---|---|---|
| CSCso50383 | Cisco IOS | Packet drops at TE/FRR tunnel disposition after node failure |
| CSCso50779 | Cisco IOS | The interface does not linkup if "speed nonegotiate" is configured |
| CSCso52097 | Cisco IOS | IPV6 :Missing second Netflow shortcut after route change |
| CSCso53557 | Cisco IOS | linecard crash @ lc_remove_vc_policy when removing and reapplying wred |
| CSCso53741 | Cisco IOS | VPNSPA does not handle duplicate IPSec SA correctly in nested tunnel |
| CSCso54131 | Cisco IOS | After SSO BPDU are being dropped |
| CSCso55072 | Cisco IOS | Crash occurs during execution of TCL code in ESM handler |
| CSCso57020 | Cisco IOS | VSS: After sso, the RBH values on orphan PO flips w/o link/po flapping |
| CSCso57886 | Cisco IOS | unrestricted while loop when looking for EOS flag in the packet |
| CSCso59288 | Cisco IOS | On enabling oob, aging is changed to 3 times is not shown in cli output |
| CSCso60063 | Cisco IOS | Router crash @ dot1x_credential_deconfig_password |
| CSCso60528 | Cisco IOS | C2W2: FWSM - Standby FWSM PO shows down and links go down eventually |
| CSCso62526 | Cisco IOS | c7600 RSP720: stdby RSP relods upon no flow-sampler interface commad |
| CSCso63263 | Cisco IOS | Bogus IPC-5-WATERMARK: 988 messages pending in xmt for the port |
| CSCso65821 | Cisco IOS | wrr-queue map configuration propagates to all ports on a 6408 |
| CSCso66357 | Cisco IOS | Classification on nbar fails on removing pmap from other pvc on ATM M2P |
| CSCso68840 | Cisco IOS | eou inactivity timer over rides reauth timer from ACS |
| CSCso69601 | Cisco IOS | Dynamic MAC address added for port in port security violation |
| CSCso71355 | Cisco IOS | PVLAN - 6500 - Multicast flood broken from pvlan port to promiscuous |
| CSCso71955 | Cisco IOS | Alignment errors with netflow on Interface, crash on 7600/6500 |
| CSCso72178 | Cisco IOS | W2:TestCapture,TestTrap & TestIPv6FibShortcut diag failed ondemand&boot |
| CSCso72250 | Cisco IOS | Incorrect color for SYSTEM led of Active and Standby sup in VS mode |
| CSCso72541 | Cisco IOS | %MFIB_STATS-DFC2-2-MFIB_STATS_LC_FAILED_GET_COUNTERS for Sip 600 |
| CSCso74559 | Cisco IOS | C2W2: Mago IOS "test Crash" create crashinfo file on bootflash only |
| CSCso74909 | Cisco IOS | Router crashes when show ip access-list <access-list-name> expand |
| CSCso81632 | Cisco IOS | Manipulating Service Module span session causes high cpu |
| CSCso82039 | Cisco IOS | C2W2: Active console is getting locked for 2.5 mins during sso. |
| CSCso84567 | Cisco IOS | 6500 with WCCP and CoPP punts non-TCP packets into CoPP policy. |
| CSCso85133 | Cisco IOS | DOM tranceiver "voltage" values are always Zero in SUP4 |
| CSCso85859 | Cisco IOS | RP crashs when using 'show memory detailed' |
| CSCso85908 | Cisco IOS | Windows client behind nat using ipsec over l2tp failed at rekey |
| CSCso86544 | Cisco IOS | Afer SSO, new active SP crashes @ pm_vlan_get_portlist |
| CSCso87083 | Cisco IOS | vtp3:crash @vlanmgr_db_get_vlist_ptr on 'test sw-vlan show nvfile' |
| CSCso87348 | Cisco IOS | Corruption in subflow code |
| CSCso87838 | Cisco IOS | HSRP: with aggressive timers HSRP peer flaps when "wr mem" |
| CSCso88042 | Cisco IOS | Wism module Allowed-Vlan statements lost on reload |
| CSCso88772 | Cisco IOS | sp-inband tx capture causes primary SUP to hang |

| Identifier | Technology | Description |
|---|---|---|
| CSCso89823 | Cisco IOS | Pos interface "rxload" and "input bytes" counters incorrectly increment |
| CSCso97593 | Cisco IOS | MCP:qos config loss after MCP reload |
| CSCso98143 | Cisco IOS | Router crash at pm_platform_private_alloc_and_reserve_vlan |
| CSCsq00884 | Cisco IOS | "mls qos trust" cmd lost under port-channel interface when upgrading IOS |
| CSCsq01879 | Cisco IOS | 7600 EoMPLS mls cef entry for imposition is programmed mtu 0 |
| CSCsq03475 | Cisco IOS | W2: Memory corruption caused by env object after being freed. |
| CSCsq04075 | Cisco IOS | C2W2:DHCP Snooping entries not cleared after removing IP Source Guard |
| CSCsq04274 | Cisco IOS | Memory leak observed on l2_vlan_stat_mem_allocate during vlans creation |
| CSCsq04355 | Cisco IOS | Fix in CSCso81632 is not complete |
| CSCsq04673 | Cisco IOS | SIGSEGV in ios-base and syslog_pubinfo_enqueue |
| CSCsq06208 | Cisco IOS | HM gold policy should not trigger again after crossing the threshold |
| CSCsq09228 | Cisco IOS | CHSTM1 SPA: Linkup/down traps not generated and snmp set not working |
| CSCsq14726 | Cisco IOS | SIP200_MP-4-TIMEOUT: Master CPU request timed out |
| CSCsq15308 | Cisco IOS | timer not stopped properly for eem policy scripts |
| CSCsq17712 | Cisco IOS | In RPR, ISSU rollback feature is broken in SRC throttle. |
| CSCsq19146 | Cisco IOS | FPD creation for new pegasus rx (1.6) FPA image for Sip-1 CR |
| CSCsq20970 | Cisco IOS | ATM option missing, while configuring T1 controller for mode atm |
| CSCsq21051 | Cisco IOS | W2: Heathland mode change doesn't work after the second SSO switchover |
| CSCsq31935 | Cisco IOS | 6500 - L3 port channel - CDP packet sent tagged in internal vlan |
| CSCsq33458 | Cisco IOS | IOS new IKE sa uses DOI of zero when ipsec sa already exists |
| CSCsq34245 | Cisco IOS | IPC Open Port Errors observed with SIP-400 |
| CSCsq36972 | Cisco IOS | Portchannel does not form. Log messages indicate misconfig. |
| CSCsq37376 | Cisco IOS | Packet Buffer Capture May Crash a 6500 in IOS |
| CSCsq39079 | Cisco IOS | SPA-IPSEC-2G Crash under load due to IKE session establishment |
| CSCsq39254 | Cisco IOS | Call-home: Standby sup reloaded after removing and adding profile |
| CSCsq41048 | Cisco IOS | Dot1x crashed at eap_peer during dot1x authentication of 350 hosts |
| CSCsq44850 | Cisco IOS | c2w2 : TB seen at %PM-3-INTERNALERROR: Port Manager Internal Software Er |
| CSCsq46327 | Cisco IOS | Ca6k SXH : 2 crypto maps in same redundant standby grp: RRI not deleted |
| CSCsq46590 | Cisco IOS | Packet loss during SSO failover on ECMP supervisor uplinks |
| CSCsq46854 | Cisco IOS | EEM applet patterns do not properly handle escape sequences |
| CSCsq47140 | Cisco IOS | 67xx module may not come online |
| CSCsq47305 | Cisco IOS | High CPU on SP when both VSL PO are source interface |
| CSCsq47774 | Cisco IOS | CDP send on internal vlan over L3 Etherchannel after reload |
| CSCsq48271 | Cisco IOS | adding redundant CSM causes config sync to indicate in sync when not |
| CSCsq51231 | Cisco IOS | ALIGN-3-SPURIOUS: Spurious memory access made @ idbman_get_port_swidb |
| CSCsq51378 | Cisco IOS | ATM PA Interface shows up/up after force redundancy, no cables connected |
| CSCsq52836 | Cisco IOS | vtp3:VLAN db is lost upon TLB(translational bridge) config |

| Identifier | Technology | Description |
|---|---|---|
| CSCsq53085 | Cisco IOS | VS: 15 seconds down time upon module reset |
| CSCsq53822 | Cisco IOS | Monitor session removal may affect traffic through WS-X6148A-RJ-45 |
| CSCsq56747 | Cisco IOS | Active SP CPU 100% after SSO switchover with 080527 Modular IOS image |
| CSCsq59297 | Cisco IOS | port-channel IDB gets mixed up |
| CSCsq60553 | Cisco IOS | Create cwslc-rommon3.bin for cwpa2 to accomodate release Rommon (1.8) |
| CSCsq61089 | Cisco IOS | VS2: physical OIR of 6708 causes 16 seconds interruption |
| CSCsq62351 | Cisco IOS | C2W2:SUPW: GOLD EEM cannot crash switch immdediately as recovery action |
| CSCsq62537 | Cisco IOS | W2: Span destination with MEC port sends duplicated traffic |
| CSCsq63041 | Cisco IOS | Unable to configure xconnect in  FE interface - command rejected |
| CSCsq63681 | Cisco IOS | c7600 Router crashing due to freed pointer in cfib invoked by Netflow |
| CSCsq64011 | Cisco IOS | VSS: Traffic from standby switch to active with RBH = 0x0 dropped |
| CSCsq67001 | Cisco IOS | Standy switch reloaded by auto qos on MEC standby member port |
| CSCsq73317 | Cisco IOS | MAB authorization failed with port-security |
| CSCsq74300 | Cisco IOS | Set interface change for CSCsk63775 needs to be backed out |
| CSCsq75704 | Cisco IOS | FW2 FE PA Interface stays up/down with no conn and goes up/up after sso |
| CSCsq77043 | Cisco IOS | EEM long hostname prevents tcl cli_open from functioning |
| CSCsq77381 | Cisco IOS | W2: Diag - TestL3Capture2 failed after LV-SSO |
| CSCsq77464 | Cisco IOS | mls rate-limit unicast cef receive value re-written upon TCAM exception |
| CSCsq78513 | Cisco IOS | VSS: Etherchannel counters incorrect |
| CSCsq78538 | Cisco IOS | ISSU: runversion/commitversion fails when specifying sup-bootdisk: |
| CSCsq78956 | Cisco IOS | strcpy of binary can cause mem corruption |
| CSCsq79253 | Cisco IOS | Pinnacle interrupts not re-enabled after memory inconsistency detected |
| CSCsq80270 | Cisco IOS | Cat 6k crashes randomly after IPSec SPA module is inserted. |
| CSCsq80891 | Cisco IOS | VSS switches reload at the same time after VSL link failure |
| CSCsq81116 | Cisco IOS | c2w2:Device crash @ oer_cc_free_message while unconfiguring |
| CSCsq81235 | Cisco IOS | Cannot configure a vrf again when deleted using 'no ip vrf' command |
| CSCsq81576 | Cisco IOS | Outcome of 'exception switch' commands may be unexpected. |
| CSCsq82663 | Cisco IOS | SLB router CPU usage is high with GE  interface |
| CSCsq82991 | Cisco IOS | IPSG Pacl entry appears after the ISSU RV or SSO |
| CSCsq83789 | Cisco IOS | LTL for unknow unicast is wrongly programmed for some L3 interfaces |
| CSCsq84116 | Cisco IOS | Cisco 7604 with OC3, Flexwan crashes into ROMMON |
| CSCsq84757 | Cisco IOS | (ha cfg-sync issue)ERSPAN config gets disabled after RP switchover |
| CSCsq85139 | Cisco IOS | VS2: Can not establish session to standby NAM |
| CSCsq89415 | Cisco IOS | "no bert" indicates "abort request" instead of "stopped" |
| CSCsq90487 | Cisco IOS | ME6524 running modular IOS images require 512 MB DRAM in SP in SXH3 |
| CSCsq91258 | Cisco IOS | L2 entry purged from hardware when in use by L3 shortcut |
| CSCsq91788 | Cisco IOS | Router crashes while loading configs ( from TFTP ) thro' VTY. |

| Identifier | Technology | Description |
|---|---|---|
| CSCsq94036 | Cisco IOS | Packets are hardware switched after applying ip precedence |
| CSCsq94068 | Cisco IOS | Archive Configuration gets out of sync when files are manually deleted |
| CSCsq94136 | Cisco IOS | Burst of traffic cause anti-replay check to fail |
| CSCsq94150 | Cisco IOS | VSS system crash on show command during the initial conversion |
| CSCsq94366 | Cisco IOS | Mem leak in rrp_update_peer_info_on_rp |
| CSCsq96843 | Cisco IOS | SIP-400 ISSU crash after inserting SPA |
| CSCsq97640 | Cisco IOS | Resetting Standby Sup4 multiple times causes lincecard switchbus timeout |
| CSCsq98887 | Cisco IOS | Packet drop on applying and removing ACL on tunnel interface with pim |
| CSCsr02723 | Cisco IOS | MDEBUG:Spurious memory access detected at env_sensor_get_update |
| CSCsr02816 | Cisco IOS | ISSU tracebacks seen on SP  during runversion at MsgReceive.S:14 |
| CSCsr06037 | Cisco IOS | the monitor session source is removed by deleting sub-interface |
| CSCsr06914 | Cisco IOS | fm_slb_inbad_send():Invalid Flowmask errors upgrading to 12.2(33)SXH2a |
| CSCsr08482 | Cisco IOS | PM support to program ethertype to all ports when port-group in mux mode |
| CSCsr08985 | Cisco IOS | CMM ports going to shutdown state on reload in Whitney 1 |
| CSCsr09554 | Cisco IOS | Move SIBYTE SB_RMON_OVRFL messages under debug |
| CSCsr12976 | Cisco IOS | High CPU in ION ios-base process |
| CSCsr13633 | Cisco IOS | %PM-3-INTERNALERROR: Port Manager Internal Software E |
| CSCsr17564 | Cisco IOS | Traceback errors seen when applying 2-level policy on a ATM VC |
| CSCsr18924 | Cisco IOS | kernel idle hook thread in IOS-Base taking 50% CPU |
| CSCsr20679 | Cisco IOS | VSL PO as SPAN source and Orphan PO as SPAN destination not allowed |
| CSCsr26663 | Cisco IOS | C2W2: GLBP  800 peers with default timers flap after SSO |
| CSCsr27735 | Cisco IOS | Tracking feature not monitor IP SLA state after boot up |
| CSCsr28305 | Cisco IOS | Packet drops on L2 portchannel on WS-X6708-10G |
| CSCsr39272 | Cisco IOS | %DATACORRUPTION-1 due to spa sensor temp overruning buffer |
| CSCsr44005 | Cisco IOS | network-rf should count virtual interfaces when calculating expected sw |
| CSCsr44967 | Cisco IOS | EEM multi-event Tcl policies fail to register |
| CSCsr45495 | Cisco IOS | PBR with deny statements : TCAM running out of masks |
| CSCsr45851 | Cisco IOS | ifOperStatus for Control Plane Interface is always down |
| CSCsr45961 | Cisco IOS | PRE2: GE ARP issue following a PRE switchover |
| CSCsr46367 | Cisco IOS | EEM mutli-event Tcl policies with all track trigger confuses EEM |
| CSCsr48938 | Cisco IOS | UNBL:bootldr image can't boot on SupW |
| CSCsr49669 | Cisco IOS | Match protcol arp doesnt work in whitney1 earlier it was working for Roc |
| CSCsr51799 | Cisco IOS | pa-mc-8t1 interface down after stopping BERT prematurely |
| CSCsr55523 | Cisco IOS | WCCP service group ID is zero in ACL TCAM Adjacency |
| CSCsr57615 | Cisco IOS | Need to add a config command to turn off/on FEFI for IOS |
| CSCsr58773 | Cisco IOS | VS2: After SSO, VSL member stuck in "w" state, and MEC errors |
| CSCsr66588 | Cisco IOS | Netflow SLB aging parameter values are not synced to SP after reload |

| Identifier | Technology | Description |
|---|---|---|
| CSCsr72427 | Cisco IOS | WS-X6148-45AF/WS-F6K-FE48-AF %ILPOWER-5-ILPOWER_MISCONFIG after reload |
| CSCsr72674 | Cisco IOS | RP crash seen @ ipmulticast_tunnel_load_split tdp_send_hello_packet |
| CSCsr75094 | Cisco IOS | MDEBUG: Spurious Memory Access on SSO |
| CSCsr78910 | Cisco IOS | time not updated in 'System returned to ROM by reload' in show version |
| CSCsr80601 | Cisco IOS | ISAKMP SA not deleted as Expected UUT |
| CSCsr81962 | Cisco IOS | C2W1: Monitor session servicemodule causes internal loop on SUP720-10GE |
| CSCsr91190 | Cisco IOS | IP multicast SSO compatibility required in images with no PIM SSO subsys |
| CSCsr93467 | Cisco IOS | c2w2:Traceback seen while doing "switch accept mode virtual " |
| CSCsr94563 | Cisco IOS | EEM: Policy fails to unregister with unkown event ID error |
| CSCsr96283 | Cisco IOS | High CPU due to add/del SPAN configs |
| CSCsr97097 | Cisco IOS | VS: RP IPC-5-WATERMARK msgs due to CARD_RESET, after SSO |
| CSCsr99560 | Cisco IOS | cos2exp policy not working for VPLS SVI after OIR |
| CSCsr99933 | Cisco IOS | FWLB: High purge rate causes CPU to increase by 15% |
| CSCsu00487 | Cisco IOS | Cat4500 MAB failure on random stack ports |
| CSCsu03297 | Cisco IOS | RE: Fabric force bus-mode does not work anymore |
| CSCsu03772 | Cisco IOS | Dot1q native vlan tagging is not working with "switchpot nonegotiate" |
| CSCsu05800 | Cisco IOS | C2W2: need to extend the wait time for bus sync after sso |
| CSCsu24825 | Cisco IOS | SUP32 unstable to communicate with all neighbors after reload |
| CSCsu27109 | Cisco IOS | When SSO is performed on 7600, mpls label allocation fails. |
| CSCsu27660 | Cisco IOS | CDP packet sent tagged in internal vlan |
| CSCsu29117 | Cisco IOS | PE send traffic back to EoMPLS tunnel after lsp path changed |
| CSCsu31444 | Cisco IOS | OER Fails to create active Jitter Probes due to IP SLA Error |
| CSCsu31651 | Cisco IOS | VSS: Traffic dropped on non-bundled port if RBH=0 |
| CSCsu33707 | Cisco IOS | Multicast traffic will not stop after PIM prune |
| CSCsu37481 | Cisco IOS | Netflow Incorrect Octet value with packet-based sampling |
| CSCsu39704 | Cisco IOS | Command "pseudowire" rejected at Virtual-PPP interface |
| CSCsu48150 | Cisco IOS | Enhancement to Me_Kr register dumps from CSCsg21809 |
| CSCsu49002 | Cisco IOS | ciscoIpMRouteBps sometimes indicates wrongful value |
| CSCsu51875 | Cisco IOS | c2w2: Router crashes at fib_upd_record_deleting |
| CSCsu55145 | Cisco IOS | ASR Crash Due To Memory Corruption |
| CSCsu57958 | Cisco IOS | DHCP-Snooping not intercepting DHCP messages from the Server |
| CSCsu59556 | Cisco IOS | Traceback seen @ fibidb_init |
| CSCsu63335 | Cisco IOS | "Failed to find process pid" error message on 12.2(33)SXH3 |
| CSCsu64581 | Cisco IOS | Last port of T3/E3 SPA connected back to back does not ping |
| CSCsu68698 | Cisco IOS | No syslogs and stack on console when SP crashes due RP boot timeout |
| CSCsu69177 | Cisco IOS | C2W2: Traffic drop after SSO on SUP4 P router w/ IP and MPLS traffic |
| CSCsu72884 | Cisco IOS | Modifying match criteria frm v6 to v4 doesnt change tcam label state |

| Identifier | Technology | Description |
|---|---|---|
| CSCsu73128 | Cisco IOS | C2W2-ION-080922: Crash on Plain IPSec tunnel setup |
| CSCsu76070 | Cisco IOS | duplicate packets when lawful intercept is enabled |
| CSCsu78109 | Cisco IOS | Intermittent HM test failures showing in SEA log |
| CSCsu94350 | Cisco IOS | C2w2:Not able to change the replication mode with latest sierra image |
| CSCsu94880 | Cisco IOS | Bus error crash at fm_format_inband_adj_data |
| CSCsu99270 | Cisco IOS | CPUHOG observed when configuring more vlan interfaces |
| CSCsv30359 | Cisco IOS | HSRP: CPU hog when no failover bound to crypto |
| CSCsv34415 | Cisco IOS | Diag failure on power-cycle puts VSS switches in rommon |
| CSCsv43802 | Cisco IOS | High CPU utilization triggers crash in diags. |
| CSCsj89931 | Voice | Standby router resets due to parser return error |
| CSCso89692 | Voice | tcl via EEM crashes IOS |
| CSCsg84658 | VPDN | CISCO-VPDN-MGMT-EXT-MIB Bad Month and Day Timestamp |
| CSCsh93436 | VPDN | L2TP in ION image may not work properly |
| CSCsi25578 | VPDN | LNS rejects L2TP ICRQ with same session ID as existing session |
| CSCsj12579 | VPDN | LAC crashes when configured with l2tp ignore tx-speed |
| CSCsj47108 | VPDN | l2tp tunnel password 7 is always in the vpdn-group config |
| CSCsk26165 | VPDN | A router may crash when configured for L2TP |
| CSCsl87404 | VPDN | L2TP tunnels are not getting established with PPPoE Relay |
| CSCsm62033 | VPDN | Call Serial Number AVP is not RFC complaint and is marked as mandatory |
| CSCso12748 | VPDN | Mandatory of Message Type AVP for SCCRQ is FALSE |
| CSCso56185 | VPDN | SCCRQ has M-bit set to 0 in Receiving Window Size AVP |
| CSCsq52048 | VPDN | Router crash with traceback decode: l2tp_l2x_cc_get_clear_cntrs |
| CSCeg65084 | WAN | FR DLCI with ppp virtual-template config is lost after reboot |
| CSCek71844 | WAN | VTEMPLATE:  Cloning from vprofile fails |
| CSCsb88464 | WAN | FR IF-MIB: ifLastChange not updated on FR/MFR encap sub Intfs (SPA/PLIM) |
| CSCsc67488 | WAN | ARP Req from Frame Relay causes %IP-4-ZERO_ADDR: Zero MAC address Error |
| CSCsg32308 | WAN | copy/paste of ntp-authentication-key statement is not possible |
| CSCsh92709 | WAN | Wrong mode being output in show users command |
| CSCsi56413 | WAN | PA-POS-OC3SMI interface output stuck . |
| CSCsj68446 | WAN | NTP will not sync - NTP packets received but ignored by NTP process . |
| CSCsl90285 | WAN | POS-APS: CWPA-3-NODISPATCH messages seen when configuring APS |
| CSCsq18856 | WAN | FR SVCs cannot be setup |

# Caveats in Release 12.2(33)SXH and Rebuilds


- Open Caveats in Release 12.2(33)SXH and Rebuilds, page 369
- Caveats Resolved in Release 12.2(33)SXH8b, page 369
- Caveats Resolved in Release 12.2(33)SXH8a, page 370
- Caveats Resolved in Release 12.2(33)SXH8, page 370
- Caveats Resolved in Release 12.2(33)SXH7, page 374
- Caveats Resolved in Release 12.2(33)SXH6, page 385
- Caveats Resolved in Release 12.2(33)SXH5, page 392
- Caveats Resolved in Release 12.2(33)SXH4, page 403
- Caveats Resolved in Release 12.2(33)SXH3a, page 413
- Caveats Resolved in Release 12.2(33)SXH3, page 415
- Caveats Resolved in Release 12.2(33)SXH2a, page 422
- Caveats Resolved in Release 12.2(33)SXH2, page 423
- Caveats Resolved in Release 12.2(33)SXH1, page 428
- Caveats Resolved in Release 12.2(33)SXH, page 441


**Note**

- The caveat information is updated frequently.
- If you have a Cisco.com account that supports access to the Bug Toolkit, you can search for the most current Release 12.2SX caveat information at this URL:

  http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

## Open Caveats in Release 12.2(33)SXH and Rebuilds

| Identifier | Technology | Description |
|---|---|---|
| CSCtb69049 | Cisco IOS | Modular IOS "exception kernel filepath ..." options are ambigous. |

## Caveats Resolved in Release 12.2(33)SXH8b

### Resolved Cisco IOS Caveats

- CSCth87458—Resolved in 12.2(33)SXH8b

  **Symptoms:** Memory leak detected in SSH process during internal testing. Authentication is required in order for a user to cause the memory leak.

  **Conditions:** This was experienced during internal protocol robustness testing.

  **Workaround:** Allow SSH connections only from trusted hosts.

  **PSIRT Evaluation:** The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2011-2568 has been assigned to

document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

### Resolved Legacy Protocols Caveats

- CSCtg48785—Resolved in 12.2(33)SXH8b

  sh x25 hunt-group causes %DATACORRUPTION-1-DATAINCONSISTENCY: copy error

## Caveats Resolved in Release 12.2(33)SXH8a

### Resolved LegacyProtocols Caveats

- CSCth69364—Resolved in 12.2(33)SXH8a

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw.

| Identifier | Technology | Description |
|---|---|---|
| CSCsw77313 | AAA | failed authentication with login command changes the logged user |
| CSCtj95352 | Cisco IOS | SUP32 resets with System NMI:**** SP System NMI: reason 0x00000009 |
| CSCtk81701 | Cisco IOS | Memory leak at "pak_pool_cache_item_get" |

## Caveats Resolved in Release 12.2(33)SXH8

| Identifier | Technology | Description |
|---|---|---|
| CSCsy61321 | AAA | tac+ acct is not failing over to next server group |
| CSCtc19317 | AAA | NAS-Port-Type set to incorrect value |
| CSCtc72862 | AAA | C2W2C: Standby router crashes at pagp_switch_mp_create_idb after SSO |
| CSCtc86306 | AAA | Authorization requests not using VRF interface |
| CSCtd16343 | AAA | Radius server declared as dead for MAB if server-private in server group |
| CSCsg49757 | Cisco IOS | Combining Gig-Sub-intf & crypto connect & vlan with crypto engine |
| CSCsg78501 | Cisco IOS | IKE should not delete established tunnel upon RSA key regeneration |
| CSCsl49350 | Cisco IOS | Console keep showing %SYS-3-CPUHOG, process =Per-minute Jobs |
| CSCsm30920 | Cisco IOS | "shutdown vlan" fails with SSO |
| CSCso59974 | Cisco IOS | BGP session goes idle after SSO switchover |
| CSCsq07729 | Cisco IOS | VSS: flowcontrol incompatible msg when standby switch port add in bundle |
| CSCsq33458 | Cisco IOS | IOS new IKE sa uses DOI of zero when ipsec sa already exists |
| CSCsr41377 | Cisco IOS | W1.3: after changing native vlan, CDP still send old native VLAN TLV |
| CSCsu52504 | Cisco IOS | %LINEPROTO-SP-5-UPDOWN msg is output when changing cdp configuration |

| Identifier | Technology | Description |
|---|---|---|
| CSCsu67919 | Cisco IOS | SIP crashes - hqf_cwpa_pak_enqueue_local |
| CSCsv82285 | Cisco IOS | Cat6k: UDP port 10000 is opened by default |
| CSCsw36363 | Cisco IOS | SUP32 temperature sensor AUX-1 temperature: N/O |
| CSCsw69621 | Cisco IOS | BR DOWN if inside bgp is only type of learning configured |
| CSCsw96176 | Cisco IOS | BFD sessions with version 0 do not come up properly following a reload |
| CSCsx24934 | Cisco IOS | CPU Monitor not heard and ipc TBs on Active VSS switch on issuing Reload |
| CSCsx56011 | Cisco IOS | Switch may crash when issuing "show mac-address-table" |
| CSCsz23099 | Cisco IOS | Memory leak due to CEF: loadinfos in Collection proc |
| CSCta56305 | Cisco IOS | Detector data port operation status not OK after boot |
| CSCta61568 | Cisco IOS | Forwarding loop after adding vlan to MST instance |
| CSCtb52180 | Cisco IOS | set vrf nvgened while vrf deletion in progress causes standby to reload |
| CSCtb65406 | Cisco IOS | QoS ACL May Not Program L4 ports Correctly In TCAM |
| CSCtb83776 | Cisco IOS | X6148A-GE-TX-Outdiscard incrementing if queue-limit of priority Q is 0 |
| CSCtc22760 | Cisco IOS | VSS ENH: Immediate reset LC after crash occurrs on stdby chassis LC |
| CSCtc28953 | Cisco IOS | Crash on cat6k running MPLS: see resolution note and CSCtc82349 |
| CSCtc30868 | Cisco IOS | Irregular CPU (peaks) on Cat6500 rtr responder |
| CSCtc39052 | Cisco IOS | svclc module command adds firewall module command to configuration |
| CSCtd18807 | Cisco IOS | "set ip next-hop <>" should lookup next hop in VRF when used on VRF int |
| CSCtd39596 | Cisco IOS | OIR of the LC causes bootup diagnostic to fail on TestL3VlanMet |
| CSCtd49505 | Cisco IOS | VSS gets to be multicast traffic blackhole after DAD or switchover |
| CSCtd64261 | Cisco IOS | LBL config sync failure for extended vlan name changes |
| CSCtd82666 | Cisco IOS | [VSS] Incorrect pMASK fpoe on standby causes traffic black-holed |
| CSCtd91871 | Cisco IOS | EZVPN - memory leak after ungraceful disconnect of client behind PATl |
| CSCte01410 | Cisco IOS | lost packests between FWSM and engine when switchover by SSO |
| CSCte15193 | Cisco IOS | c2w2c:"no spanning-tree vlan 16" command is not removed from standby |
| CSCte21190 | Cisco IOS | WS-X6148A-GE-TX ports 25-32 stop forwarding traffic |
| CSCte40472 | Cisco IOS | FWSM: Private vlan association not syncing on VSS systems from switch |
| CSCte43407 | Cisco IOS | No %LINK-3-UPDOWN log for SPAN destination port |
| CSCte48967 | Cisco IOS | VSS : isolated pvlan not associated with VRF on DFCs |
| CSCte56437 | Cisco IOS | TCP connection loss due to NAT incorrect translation on cat6500 |
| CSCte72214 | Cisco IOS | ME6500 - Traffic may be dropped on applying cos-map. |
| CSCte79217 | Cisco IOS | ICCQ never decreases, flow stats affected, (S,G) expires |
| CSCte81230 | Cisco IOS | IP Source Guard feature goes into an incorrect state |
| CSCte83052 | Cisco IOS | Xauth is getting disabled when putting keyring into isakmp profile12.2 |
| CSCte89428 | Cisco IOS | SNMP tty traps not sent |
| CSCte90261 | Cisco IOS | 6500 PoE issues with 1120 and 1230 line of APs when using dot1x |
| CSCte99373 | Cisco IOS | extranet: mrib S,G entry never removed after pim disabled on IIF |

| Identifier | Technology | Description |
|---|---|---|
| CSCtf02760 | Cisco IOS | Kernel crash (cache error) without any crashinfo generated |
| CSCtf12634 | Cisco IOS | SXH:idb->vlan_id on RP not getting updated on trunk native vlan change |
| CSCtf18863 | Cisco IOS | REDZONEERROR and crash seen on SXH6 after install operation |
| CSCtf37626 | Cisco IOS | Ospf flaps with oversubscription on enhanced flexwan Multilink T1 |
| CSCtf39183 | Cisco IOS | OBFL Master may not be initialized after IOS upgrade from SXF to SXH |
| CSCtf51541 | Cisco IOS | Mistral reset due to TM_DATA_PARITY_ERROR error |
| CSCtf52407 | Cisco IOS | Sup720 may reload when passing GRE traffic |
| CSCtf54617 | Cisco IOS | Supervisor fails to come up due to bad compact flash. |
| CSCtf62507 | Cisco IOS | Netflow s/w switched flow not entried if disable/enable ip flow ingress |
| CSCtf91692 | Cisco IOS | Insertion of 6708/6716 linecard into the chassis resets another linecard |
| CSCtf97963 | Cisco IOS | VSS DFC card miss MN setting, 4Sup: ICS MN ORPOE error |
| CSCtg37826 | Cisco IOS | Inter range command doesn't work |
| CSCtg55075 | Cisco IOS | IOS SLB may not purge netflow shortcut properly |
| CSCtg58235 | Cisco IOS | Minor Error @ bootup on multiple 8xCHT1/E1 SPA cards. |
| CSCtg68012 | Cisco IOS | %SCHED-3-THRASHING: Process thrashing on watched mssg event |
| CSCtg73213 | Cisco IOS | c2w2c - Crash seen on Configuring ATMoMoGRE |
| CSCtg78883 | Cisco IOS | Patch triggers EARL Recovery. |
| CSCth04998 | Cisco IOS | [VSS] DFC installs drop index for MAC-address |
| CSCth13572 | Cisco IOS | C2W2C: WS-X6716-10GE Failed TestMacNotification and reset after VSS SSO |
| CSCth23794 | Cisco IOS | interfaces errdisable with "vlan intern alloc policy descending" config |
| CSCth42223 | Cisco IOS | DOT1X security violation message not report the interface mode |
| CSCth46650 | Cisco IOS | Traffic not get through between promiscuous and isolated in Mux mode |
| CSCth55383 | Cisco IOS | %EARL-DFC2-2-SWITCH_BUS_IDLE message after "show tech" |
| CSCth60232 | Cisco IOS | SXH: Port-channel interface flap when changing vlan mask |
| CSCth76204 | Cisco IOS | TestSPRPInbandPing - No swover/crash after failure threshold reached |
| CSCti23872 | Cisco IOS | traceroute double hop with set vrf due to double ttl decrement |
| CSCti36394 | Cisco IOS | SXH Firmware - Heathland Board Layer Test Error Counter Monitor |
| CSCti84718 | Cisco IOS | CPUHOG @ ipnat_ipalias_check_waitlist+E8 after sh/nosh PBR po int |
| CSCti85352 | Cisco IOS | W1.8: Removing vlan-group from fw mod,vlan-gp already assign get removed |
| CSCsh47251 | Infrastructure | 3700 crashes as soon as loading image |
| CSCsl05310 | Infrastructure | %SCHED-3-STUCKMTMR tb's seen with 1022 ION |
| CSCsy24505 | Infrastructure | Process "sbin/dfs_disk0.proc" crashed while inserting CF @ dfs_id_delete |
| CSCtc87480 | Infrastructure | dir slavenvram and wr mem triggers slavenvram:/(Device or resource busy) |
| CSCtd62220 | Infrastructure | %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, |
| CSCte52416 | Infrastructure | VSS member switch crash when power down active switch |
| CSCtg19572 | Infrastructure | Memory leak in two dfs processes |
| CSCtg64468 | Infrastructure | indefinit loops in get_bufferpool_info() & get_buffercachepool_info() |

| Identifier | Technology | Description |
|---|---|---|
| CSCth01674 | Infrastructure | *Dead* memory increasing in (coalesced) |
| CSCsa94774 | IPServices | NAT default breaks Traceroute response |
| CSCsy74796 | IPServices | Memory leak at ip_multicast_ctl (when creating/deleting interfaces?) |
| CSCsz05783 | IPServices | NAT translation fails with certain ALG traffic |
| CSCta56667 | IPServices | tcp.proc displays excessive cpu usage |
| CSCtd21890 | IPServices | Router crash at dhcp autoinstall |
| CSCtf34691 | IPServices | HSRP group name tied to static NAT for redundancy is not saved to config |
| CSCsk98507 | LegacyProtocols | Device crash@novell_send_gen_rip_query . |
| CSCte78230 | LegacyProtocols | DLSw Ethernet Redundancy and IPV6 will not work together |
| CSCta48816 | Management | CDP Protocol: %SYS-2-GETBUF: Bad getbuffer, bytes= 32717 |
| CSCtc90579 | MPLS | Block allocated by 'rsvp_hc_db_nbr_alloc' gets corrupted |
| CSCth36724 | MPLS | Router reload while unconfiguring vrf interfaces in HA scale tests |
| CSCth38699 | Multicast | Auto-RP for multicast triggers RP-Discovery with 0 RPs |
| CSCso26773 | QoS | qos: PI-code: police percent above 43% is not correct for 10G interface |
| CSCsu99767 | Routing | EIGRP:peer does not send UPDATE to NSF/SSO restarting peer router |
| CSCtc72772 | Routing | Bulk sync failure and Standby reloads continuously @ "clns route" |
| CSCtd49246 | Routing | round-trip average of ping MIB may show less value |
| CSCtd81664 | Routing | Not possible to "set ip next-hop" in vrf with import-map |
| CSCtf06436 | Routing | high CPU due to HW backwalk continually walking the looped OCE chain |
| CSCtf28793 | Routing | bgp aggregate-address suppress-map does not suppress specific prefixes |
| CSCtf64231 | Routing | Inbound route-map change shouldn't be effective immediately |
| CSCtg27206 | Routing | Static route not redistributed by RIP after link flap |
| CSCsb10291 | Security | $$TS: Router forced crash on PKI Bind service failure (C_UnbindService) |
| CSCsf17411 | Security | trustpoint authentication fails if key usage is non standard |
| CSCsk22496 | Security | Router crashes @ssh_command when remoove crypto key |
| CSCsv86113 | Security | SSH on VRF int is allowed irrespective of vrf-also key |
| CSCsv92274 | Security | SSH process might not handle some IPC messages |
| CSCsz05583 | Security | crypto pki config nvgened before ip config on which it depends - slow |
| CSCta77073 | Security | Router Crash while unconfiguring crypto trustpoint |
| CSCtf47512 | Security | SXH5: Memory leak in ACE HAPI and IPSec Key Engine |
| CSCtg11808 | Security | VSS: Standby supervisor reloads when crypto pki trustpoint removed |
| CSCti26768 | Security | Bus error while re-configuring a trustpoint |
| CSCtd22993 | WAN | SNMP ifIndex for certain serial interfaces becomes inactive |
| CSCtf03928 | WAN | NTP packets received but ignored by the NTP process |

## Caveats Resolved in Release 12.2(33)SXH7

### Resolved AAA Caveats

- CSCsg21398—Resolved in 12.2(33)SXH7

  **Symptoms:** The Cisco IOS software image may unexpectedly restart when a crafted "msg-auth-response-get-user" TACACS+ packet is received.

  **Conditions:** This symptom is observed after the Cisco platform had send an initial "recv-auth-start" TACACS+ packet.

  **Workaround:** There is no workaround.

### Resolved Multicast Caveats

- CSCsl32142—Resolved in 12.2(33)SXH7

  **Symptoms:** A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with 'Bad getbuffer' error may also be reported.

  **Condition:** Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

  **Workaround:** Configure IP multicast boundary without the **filter-autorp** option.

- CSCtc68037—Resolved in 12.2(33)SXH7

  **Symptom:** A Cisco IOS device may experience an unexpected reload as a result of mtrace packet processing.

  **Conditions:**

  **Workaround:** None other than avoiding the use of mtrace functionality.

### Resolved Security Caveats

- CSCsz32366—Resolved in 12.2(33)SXH7

  **Symptoms:** A Cisco router that is running Cisco IOS Release 12.4(25) may crash due to SSH.

  **Conditions:** This symptom occurs when SSH is enabled on the router. An attempt to access the router via SSH is made.

  **Workaround:** Do not use SSH. Disable SSH on the router by removing the RSA keys:

  "crypto key zeroize rsa"

  Further Problem Description: This issue has not been seen in Cisco IOS Release 12.4(23) and earlier releases. It also has not been seen in Cisco IOS Release 12.4T images.

- CSCsg65318—Resolved in 12.2(33)SXH7

  **Symptoms:** Malformed SSH version 2 packets may cause a memory leak.

  **Conditions:** This symptom is observed on a Cisco platform configured for SSH version 2 after it has received malformed SSHv2 packets. The impact of this flaw is that the affected platform may operate in a degraded condition. Under rare circumstances it may reload to recover itself.

  **Workarounds:** Options consist of using SSH version 1 in the interim until the affected platform can be upgraded to a fixed release or permitting only known trusted hosts/networks that can connect to the router by using a VTY access list.

  **Following are examples of the workarounds:**

  Configure SSH version 1

  ```
  Configure SSH version 1
  ```

```
+----------------------
 !-- configure from global config mode
 !
 config t
 !
 ip ssh version 1
 end

VTY access-list
+--------------
 !-- 10.1.1.0/24 is a trusted network that
 !-- is permitted access to the router, all
 !-- other access is denied
 !
 access-list 99 permit 10.1.1.0 0.0.0.255
 access-list 99 deny any
 !
 line vty 0 4
  access-class 99 in
 end
```

More information about configuring VTY access lists is available in Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T Controlling Access to a Virtual Terminal Line:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/12-4t/sec-cntrl-acc-vtl.html

More information about SSH on IOS is available in the Configuring Secure Shell on Routers and Switches Running Cisco IOS guide:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

### Resolved Unknown Caveats

- CSCtc41760—Resolved in 12.2(33)SXH7

  **Symptom:** 6500 may experience redzone crash at UDLD process. Message may appear %SYS-SP-3-OVERRUN: Block overrun at 44456570 (red zone 6D000700) -Traceback= 40291448 402938DC 40D74570 40D763A0

  Traceback will vary from code to code.

  **Conditions:** UDLD configured

  **Workaround:** Disable UDLD.

- CSCtc49782—Resolved in 12.2(33)SXH7

  **Symptoms:** Upgrade from 12.2(18)SXF6 to 12.2(33)SXH5 introduced additional vty lines to the running-configuration (vtp line 5 - 15). These new lines do not inherit the security ACL or transports configured by the customer on the old lines (0-4). Switch upgrade caused device to be non-compliant with network security policy defined by customer.

  **Condition:** Software upgrade from 12.2(18)SXF6 to 12.2(33)SXH5.

  **Workaround:** We have to manually configure the ACL for those newly introduced vty lines.

- CSCtc71597—Resolved in 12.2(33)SXH7

  **Symptom:** Currently in EARL7 system, For an IPv6 packet the 96 bytes cover DBUS header (22), Ether header (14), IPv6 harder (40), IPv6 extension headers, and L4 header. That means only 20 bytes (96 - 22 - 14 - 40) are for extension header(s) and L4 header. So even packet with small extension header(s) can use up to 20 bytes that would cause l4_hdr_vld = 0. When that happens, all L4 features cannot be applied and packet would be hardware forwarded based on L3 forwarding result.

**Conditions:** This issue is present from day one but would cause threat only when ipv6 access-list is configured on any interface and that access-list is containing L4 options.

**Workaround:** No Workaround

- CSCte83104—Resolved in 12.2(33)SXH7

  **Conditions:** When an ipv6 RACL is confiured on an interface. All packets containing ipv6 optional headers are punted to RP. But if any packets that are sent with no L4 header are also hitting this punt entry present at the top of tcam.

  **Workaround:** No Workaround:

- CSCsh61458—Resolved in 12.2(33)SXH7

  **Symptoms:** A Cat4k switch may reload after receiving a malformed packet on one specific specific port.

  **Conditions:** This symptom may be observed on a Cat4k switch that enables DNSIX audit trail and recieves crafted IP packets on a specific port.

  **Workaround:** Do not enable the DNSIX audit trail.

### Resolved WAN Caveats

- CSCtd75033—Resolved in 12.2(33)SXH7

  **Symptom:** Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability. Note: The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section **Further Description** of this release note enclosure.

  **Conditions:** Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

  This is the same as the vulnerability which is described in http://www.kb.cert.org/vuls/id/568372

  Cisco has release a public facing vulnerability alert at the following link:

  http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

  Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

  All other versions of Cisco IOS and Cisco IOS XE Software are affected.

  To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

  The following example identifies a Cisco device that is configured with NTP:

```
router# show running-config | include ntp
ntp peer 192.168.0.12
router#
```

  The following example identifies a Cisco device that is not configured with NTP:

```
router# show running-config | include ntp
router#
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>
```

The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router# show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

http://www.cisco.com/web/about/security/intelligence/ios-ref.html

**Workaround:** There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

**Note:** NTP peer authentication is not a workaround and is still a vulnerable configuration.

- NTP Access Group

  **Warning:** Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

  ```
  !--- Configure trusted peers for allowed access
  access-list 1 permit 171.70.173.55
  !--- Apply ACE to the NTP configuration
  ntp access-group peer 1
  ```

  For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

- Infrastructure Access Control Lists

**Warning:** Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well.  The following example covers
!---   an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.

access-list 150 deny udp any
INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example
!--- shown)

interface fastEthernet 2/0
   ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

– Control Plane Policing

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

—Filtering untrusted sources to the device.

**Warning:** Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
   any eq 123

!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 123

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
   match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
   class drop-udp-class
      drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
   service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

—Rate Limiting the traffic to the device The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

**Warning:** If the rate-limits are exceeded valid NTP traffic may also be dropped.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
   match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates

policy-map rate-udp-traffic
   class rate-udp-class
      police 10000 1500 1500 conform-action transmit
         exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
   service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

**Further Description:** Cisco IOS Software releases that have the fix for this Cisco bug ID, have a behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message: Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command **ntp allow mode private** should be configured. This is disabled by default.

#### Other Resolved Caveats in Release 12.2(33)SXH7

| Identifier | Technology | Description |
|---|---|---|
| CSCsi54201 | AAA | IDMGR-3-INVALID_ID error message |
| CSCsq71492 | AAA | IOS device crash or tracebacks at tplus_handle_req_timeout |

| Identifier | Technology | Description |
|---|---|---|
| CSCsx15897 | AAA | Cisco 3800 shows symptoms of memory leak in AAA component |
| CSCsy55362 | AAA | Unresponsive Console/VTYs |
| CSCtc27153 | ATM | Shaping configuration does not work in SXH |
| CSCsb95192 | Cisco IOS | RRI with HA doesnt populate the routes correctly - static keyword |
| CSCsk18794 | Cisco IOS | speed and negotiation configuration issue on FE-TX-V2 SPA |
| CSCsk49041 | Cisco IOS | crypto_ikmp_utils.c: possible Invalid Pointer Read |
| CSCsk66851 | Cisco IOS | *,G/m entry does not have OIF programmed in HW sometimes |
| CSCsk86410 | Cisco IOS | Abnormal ISAKMP traffic caused an alignment error and traceback. |
| CSCsl30308 | Cisco IOS | PIM snooping corrupts PIM RPF Proxy packet |
| CSCsl70542 | Cisco IOS | OBFL:high cpu during interrupt coalesce |
| CSCsl87677 | Cisco IOS | changing the access vlan doesn't reflect the vlan of the secure configur |
| CSCsm40013 | Cisco IOS | Multiple LC crash after shuting down TE tunnel interface |
| CSCsm63524 | Cisco IOS | SUP32 crashes due to SP hang when it recovers from errdisable |
| CSCsm96309 | Cisco IOS | OIR-SP-4-WARN message displayed when PS1 or FAN removed |
| CSCsq01879 | Cisco IOS | 7600 EoMPLS mls cef entry for imposition is programmed mtu 0 |
| CSCsq63621 | Cisco IOS | SPD classifies OSPF IP Precedence 0 as priority |
| CSCsr09586 | Cisco IOS | Remarks not appearing correctly in Policy Based ACL |
| CSCsr50134 | Cisco IOS | Router or Linecard may reload at cv6_6pe_frr_stats |
| CSCsr74002 | Cisco IOS | 7600 - VPLS - QinQ- UDLD packet received on qinq flooded to vpls |
| CSCsu31088 | Cisco IOS | Not able to execute any commands under intf after running SPA FPGA bert |
| CSCsu72935 | Cisco IOS | C2W2B: memory corruption on 122-32.8.11.XIW20 (w2_x_pi) image |
| CSCsu84213 | Cisco IOS | RPF-MFD hardware entry is missed after doing SSO. |
| CSCsu99813 | Cisco IOS | C2HD1-SI:Span Distributed Stops Traffic - Centralized Duplicates |
| CSCsv13243 | Cisco IOS | BFD config causing BGP session to go down |
| CSCsv40523 | Cisco IOS | WISM: Gig interfaces show as unknown(4) |
| CSCsv43187 | Cisco IOS | 120seconds after SSO, Some multicast traffic drops |
| CSCsw40790 | Cisco IOS | SNMP Loop on PA-MC-T3+ interfaces (Installed) |
| CSCsx65705 | Cisco IOS | router crash on no route-map with match ipv6 address access-list |
| CSCsx74064 | Cisco IOS | On modular IOS, SSH on VRF int is allowed irrespective of vrf-also key |
| CSCsx79379 | Cisco IOS | IOS Auth Proxy HTTP may lead to bus error adress 0x0 |
| CSCsy04594 | Cisco IOS | Vlan interfaces flap when a root guard port receive superior bpdu |
| CSCsy37236 | Cisco IOS | High CPU  at Filesys process on DFC LC and crash at btree_map_search |
| CSCsy54583 | Cisco IOS | TTY data process on DFC leaks memory at prot_tty_malloc_named |
| CSCsy56433 | Cisco IOS | Sh rom intermittently fails to display correct region info for standby |
| CSCsy58553 | Cisco IOS | Linecard reset causes traffic onto frr protected tunnel to be dropped |
| CSCsy66446 | Cisco IOS | %BIT-SP-4-OUTOFRANGE ltl_fpoe_defer_notify_with_pri on port-channel flap |
| CSCsy66678 | Cisco IOS | stp_helper_manipulate_queue: standby SP CPUHOG |

| Identifier | Technology | Description |
|---|---|---|
| CSCsy81934 | Cisco IOS | Non-standard static multicast MAC addresses lose ports after reload |
| CSCsy86252 | Cisco IOS | SP Crash printing "supervisor jamming EOBC.  It will be disabled." |
| CSCsz04297 | Cisco IOS | Cat6k: False Dynamic MAC entry is installed with format 0000.<LTL>.0000 |
| CSCsz19246 | Cisco IOS | Crash after 'no dot1x port-control auto' |
| CSCsz36826 | Cisco IOS | 6509E fan-tray failed to restore back to HP mode after OIR |
| CSCsz38798 | Cisco IOS | On SSO, Sup engine/DFC module get reset when MET set deleted |
| CSCsz53124 | Cisco IOS | IPSEC VPN interoperability issue  when IPCOMP compression enabled |
| CSCsz53809 | Cisco IOS | Configuring vlan name containing space doesnt work across reload. |
| CSCsz69993 | Cisco IOS | Pause frames on WS-X6708-10GE sent to cpu with flow-control disabled |
| CSCsz96469 | Cisco IOS | Tracebacks seen @chunk_free_with_pc while unconfiguring |
| CSCta06428 | Cisco IOS | VSS: Active Crash at iccp_test_get_first_mcast_resp_data |
| CSCta06451 | Cisco IOS | PfR:BR Memory leak in export path on 7600 |
| CSCta15851 | Cisco IOS | Changing allowed vlan mask causes WiSM LAG member ports to reset |
| CSCta29818 | Cisco IOS | Enhanced-Flexwan Module Power Down after Code Upgrade from SXF to SXH |
| CSCta42669 | Cisco IOS | C2W1: segv exception after portchannel configuration |
| CSCta45976 | Cisco IOS | BFD adj not formed if NBR IPaddr is on the same RTR but w diff VRFintf |
| CSCta56676 | Cisco IOS | IPsec SA liftime can go to negative values |
| CSCta56890 | Cisco IOS | WiSM LAG and Data Ports flaps on SSO Switchover |
| CSCta71873 | Cisco IOS | Mcast traffic stops flowing across fabric to required fpoes |
| CSCta95295 | Cisco IOS | IOMEM depleted when PKI servers unavailable for CRL checking |
| CSCta98108 | Cisco IOS | With NAT, on Netflow database cleanup timer expiry, CPU spikes on 7600 |
| CSCtb04231 | Cisco IOS | Imprecise parity error crash due to mistral timeout |
| CSCtb31400 | Cisco IOS | BGP sends Route-Refresh request on entering route-map configuration |
| CSCtb45475 | Cisco IOS | sh plat hard capacity cpu report system memory usage incorrectly |
| CSCtb62031 | Cisco IOS | cat6k: High cpu and high inband when reflexive ACL is used with WCCP |
| CSCtb70578 | Cisco IOS | L2PT incorrectly decapsulates  STP PDU for RSPAN causing PVID mismatch |
| CSCtb72638 | Cisco IOS | Ezvpn server not sending split tunneling access-list to client |
| CSCtb78973 | Cisco IOS | PM-SP-3-INTERNALERROR: Port Manager Internal Software Error with dot1x |
| CSCtb84298 | Cisco IOS | Shadow state of wism PO line protocol down on stdby After OIR of WiSM |
| CSCtb87149 | Cisco IOS | NF is disabled on L3 sub-intf with per interface NF enabled |
| CSCtc11691 | Cisco IOS | VSS: Switch crashes after loading the sierra 090920 image |
| CSCtc15386 | Cisco IOS | IOS tags VLAN name configuration command as level 1 |
| CSCtc16740 | Cisco IOS | Global BPDUGuard does not work on MVAP ports |
| CSCtc17058 | Cisco IOS | VC stops sending traffic due to duplicate vpn id in port based EoMPLS |
| CSCtc22217 | Cisco IOS | SPA-8X1FE-TX-V2 negotiation auto and duplex mode issue |
| CSCtc24864 | Cisco IOS | Enable cdp - removed on shut/ no shut dot1q-tunnel interface |
| CSCtc27745 | Cisco IOS | LLDP packets go out tagged if native vlan (not Vlan1) is configured |

| Identifier | Technology | Description |
|---|---|---|
| CSCtc30691 | Cisco IOS | Crash/Spurious memory access on privilege ipaddr-object-group/port-objec |
| CSCtc38716 | Cisco IOS | ME6524 may reset due to single power supply failure |
| CSCtc38771 | Cisco IOS | 12.2SXH: Intermittent BPDU drop over Dot1Q tunnel. |
| CSCtc40724 | Cisco IOS | Multicast packets may get dropped on 6500 when member join mcast group |
| CSCtc40851 | Cisco IOS | traceback on applying port acl to interface. |
| CSCtc49542 | Cisco IOS | VSS: output drops on VS-720 port due to CoS mapping mismatch |
| CSCtc52807 | Cisco IOS | C2HD1-SI: L3 Portchannel's FPOE mask incorrect after SSO |
| CSCtc53958 | Cisco IOS | "sh run" on Cat6k results in tunnel flapping on non-modular IOS |
| CSCtc79335 | Cisco IOS | Sup Crash on several locations with IP SEC config |
| CSCtc81772 | Cisco IOS | High cpu utilization with IPv6 ACL |
| CSCtc90469 | Cisco IOS | Sup32 crash just after boot up with ACL Deny Test Failure |
| CSCtd01483 | Cisco IOS | With fm platform debug on when private-host is config'd the switch crash |
| CSCtd13853 | Cisco IOS | Linecard interfaces going into UDLD errdisable state on reload |
| CSCtd16863 | Cisco IOS | 6500 PoE issues with 1120 line of APs when using dot1x |
| CSCtd18947 | Cisco IOS | Port-based EoMPLS stops passing tagged traffic |
| CSCtd21153 | Cisco IOS | Packets are not netflow switched for wccp-L2-redirect(inbound)with hash |
| CSCtd31143 | Cisco IOS | SPA in CC mode with SSO breaks connectivity when other sup comes online |
| CSCtd35521 | Cisco IOS | MVPN PIM neighborship is not formed within vrfs |
| CSCtd45736 | Cisco IOS | EOAM:LB functionality is broken from 11/17 due to CSCtb70578 |
| CSCtd58314 | Cisco IOS | memory corruption crash with sh ip arp inspect log |
| CSCtd59572 | Cisco IOS | Spurious memory access errors seen after fpd upgrade of T3/E3 on SIP200 |
| CSCtd59664 | Cisco IOS | %ERROR: Standby doesn't support this on configuring speed on SIP-400 int |
| CSCtd72437 | Cisco IOS | Packets punted to software forwarding when route-map is used for NAT |
| CSCtd78587 | Cisco IOS | Crash when recovering a port which was err-disabled twice |
| CSCtd92043 | Cisco IOS | Ph2 rekey use wrong proxy-id's on cat6k ezvpn ipsec-spa-2g |
| CSCte08785 | Cisco IOS | mac notification change history log not seen for deleted mac entries. |
| CSCte20914 | Cisco IOS | SPAN Reflector not enabled for WS-SVC-ADM-1-K9 : 2nd Commit |
| CSCte56366 | Cisco IOS | DSCP values are not mapped to RX priority queue |
| CSCte87347 | Cisco IOS | FPGA upgrade of CHT1E1 to 2.8 is not successful |
| CSCtf03547 | Cisco IOS | VSS: Switch went down coz %EARL-SW1_SP-4-EBUS_SEQ_ERROR: with SXH7 image |
| CSCtf06477 | Cisco IOS | VSS: changing switching mode powers down service modules in SXH |
| CSCtf16330 | Cisco IOS | DHCP Rogue Server Detection : Multiple DHCPDISCOVER's issue |
| CSCtf53433 | Cisco IOS | Knob 'platform ipv6 acl punt extension-header' default should be false |
| CSCei86912 | Infrastructure | Router reloads unexpectedly while issuing GD commands |
| CSCin66315 | Infrastructure | Inconsistency with sysuptime and rttMonLatestRttOperTime |
| CSCsj27963 | Infrastructure | Need graceful handling of full nvram |
| CSCsk85192 | Infrastructure | copy command with : after attribute is not checked against ACS. . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl52962 | Infrastructure | interface range Port-channel command causes RP crash |
| CSCsm80522 | Infrastructure | Zero size crash file generated with "test crash" on Sip 600 module |
| CSCso40612 | Infrastructure | 7600 HA router crashed @ parser_syntax_cleanup on |
| CSCso48834 | Infrastructure | ip sla config with udp-jitter probe failed due to no connection |
| CSCso56916 | Infrastructure | persistent variable "snmpboot" don't get incremented after reload |
| CSCse59109 | IPServices | high CPU usage when IP SLA is enabled |
| CSCsi99841 | IPServices | vrf-aware trustpoint authentication/enrollment doesn't work |
| CSCsm52759 | IPServices | % Internal software error: 22 seen on telnetting to ipv6 hosts |
| CSCsz72591 | IPServices | Router configured as a DHCP client crashes with crafted DHCP packet. |
| CSCsz97239 | IPServices | PmtuAger Expiration and MSS value |
| CSCtc55616 | IPServices | RSA key generation from SSH session disables SSH service in ION |
| CSCtd13820 | IPServices | Show Standby causes unexpected exception to CPU: crash at standby_show |
| CSCtd32285 | IPServices | No nat translation with PAT applied on VRF interfaces |
| CSCsc62963 | LAN | Have configurable MTU Range 1500 -1530 on PA-1FE and PA-2FE |
| CSCsz05918 | Management | CDP neighbors do not come up on vlan interface |
| CSCsz75221 | Management | A local variable in cdp takes up 2k process stack space-prompting crash |
| CSCtc40711 | Management | next-hop verify-availability still forwards traffic with no CDP neighbor |
| CSCtd43540 | Management | Memory leak at cdp_handle_version_info |
| CSCtb76828 | Multicast | %SYS-2-BADSHARE: Bad refcount in datagram_done for MSDP process |
| CSCsm42477 | QoS | Sierra:Standby reloaded on QOS configuration. |
| CSCso29025 | QoS | Sip-400: Traceback msgs at process_ok_to_reschedule |
| CSCsq11897 | Routing | Spurious memory seen at idb_get_ip_addrs and idb_get_ip_unnum |
| CSCsq13111 | Routing | 7609s vlan traffic reporting |
| CSCsq99447 | Routing | When BFD/ EIGRP configured in more than 32 vrf BFD does not come up |
| CSCsr05431 | Routing | After SSO, cef removed vrf routes before bgp graceful timers time-out |
| CSCsr67177 | Routing | Router with IPv6 OSPF crashes on reloading |
| CSCsr84530 | Routing | Static route not properly redistributed into BGP -- backout CSCsl92283 |
| CSCsr88705 | Routing | BGP route getting lost after "shut/no shut" of BGP peering interface |
| CSCsw30941 | Routing | ospfNbrStateChange trap sent by non-DR |
| CSCsw99768 | Routing | BGP malformed update sent |
| CSCsy58115 | Routing | Continuous BGP mem increase with non established neighbors |
| CSCsz61156 | Routing | NH is not stored in BGP table when IPv6 VRF is redistributed |
| CSCta07104 | Routing | Config-Sync & Traffic failure in VPN SSO scripts |
| CSCta08632 | Routing | ISIS topology broken after Sup force-switchover with ispf |
| CSCtb82674 | Routing | IS-IS adjacency stays down after switchover |
| CSCtc45716 | Routing | SNMPWALK of ipRouteEntry.7 with a view configured triggers high CPU |
| CSCtd73256 | Routing | a catalyst switch may reload unexpectedly during 'show ip ospf int' |

| Identifier | Technology | Description |
|---|---|---|
| CSCte10790 | Routing | c6500: device crashing on "no 250" on access-list |
| CSCse31829 | Security | Memory leak in Crypto IKMP process |
| CSCsz83570 | Security | SSH Sessions disconnect when viewing logs w/ pagers |
| CSCtc12312 | Security | PKI may get stuck after 32678 CRL fetches |
| CSCsi05069 | WAN | DCE Sub-interface is not coming up after provisioning |
| CSCsw31019 | WAN | Router crashes while configuring the command "frame-relay be 1" |

## Caveats Resolved in Release 12.2(33)SXH6

### Resolved MPLS Caveats

- CSCsz45567—Resolved in 12.2(33)SXH6

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

### Resolved Routing Caveats

- CSCsv30595—Resolved in 12.2(33)SXH6

  **Symptoms:** Cisco IOS device may crash.

  **Conditions:** A Cisco IOS device may crash upon receiving a malformed OSPF message.

  Before the issue can be triggered, the Cisco IOS device must be able to establish adjacency with an OSPF peer. The issue will then occur when the processing an OSPF message sent by the peer.

  **Workaround:** There is no workaround. Using OSPF authentication can reduce/minimize the chance of hitting this issue.

### Resolved Security Caveats

- CSCsx70889—Resolved in 12.2(33)SXH6

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels

### Resolved Unknown Caveats

- CSCsy07555—Resolved in 12.2(33)SXH6

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ipsec

- CSCsy15227—Resolved in 12.2(33)SXH6

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy

### Other Resolved Caveats in Release 12.2(33)SXH6

| Identifier | Technology | Description |
|---|---|---|
| CSCin67182 | AAA | Crash in aaa_sg_v2_get_next_server on trying unconfigured radius ser |
| CSCsc97727 | AAA | Access Point Crashes When Removing TACACS Server |
| CSCse12395 | AAA | Check keys error for accounting does not cause failover |
| CSCsh34529 | ATM | autobahn76: ATM interface config lost on standby RP |
| CSCsx43905 | ATM | Router Crash at dlcncia.c on 12.2(33.4.14)SXH |
| CSCee25454 | Cisco IOS | SADB peering process leaks memory after overnight test |
| CSCek53099 | Cisco IOS | SIP200+4xT3/E3:Fail to load cRTP CFG from startup file |
| CSCsd39568 | Cisco IOS | stats support for PBR set ip nexthop/set interface |
| CSCsg35285 | Cisco IOS | Slower Cache refresh for int stats when more interfaces up |
| CSCsi46897 | Cisco IOS | PRE crash after snmpwalk on mib cbQosSetStatsTable |
| CSCsj26698 | Cisco IOS | Acct-Session-Id in Accounting-Request is different from in Access-Reques |
| CSCsk25046 | Cisco IOS | Not all ifIndex'es are in cbQosServicePolicyTable |
| CSCsk29975 | Cisco IOS | Tunnel not up, invalid local address after modify the local address . |
| CSCsk62407 | Cisco IOS | CPU HOG@fm_format_addr_to_compare on applying large IPv6 ACL |
| CSCsl61273 | Cisco IOS | Standby crash after autoqos config |
| CSCsl72962 | Cisco IOS | Mask the debug message error in multicast throttle logic |
| CSCsm39160 | Cisco IOS | TestCFRW shows incorrectly as failed in show diagnostic sanity |
| CSCsm45254 | Cisco IOS | OBFL ENV app in infinite-loop causing high CPU |
| CSCsm84073 | Cisco IOS | c2w2:vrf ping fails after toggle mls mpls recir, sso,remove/add ip vrf |
| CSCsm84163 | Cisco IOS | Memory leak for IKE/IPSEC after hsrp failover, router crashed w/ no mem |
| CSCso35876 | Cisco IOS | SRB3:New active SP crash at label_entry_get_inlabel |

| Identifier | Technology | Description |
|---|---|---|
| CSCso36150 | Cisco IOS | duplicate vlan names causing config-sync failures |
| CSCso59242 | Cisco IOS | sierra: show mem detailed all stat is truncated. |
| CSCso79925 | Cisco IOS | EC with enhanced hash method (PFC3C) has no knob to use old method (3B) |
| CSCso89644 | Cisco IOS | c2w2::Missing idb for fibidb NDE_vlan1019 messages and tracebacks after |
| CSCsq31935 | Cisco IOS | 6500 - L3 port channel - CDP packet sent tagged in internal vlan |
| CSCsq55506 | Cisco IOS | Inter community PVLAN traffic is software switched |
| CSCsq69567 | Cisco IOS | SSO Switchover + unicast-routing chg cause MC traffic loss for 2 minutes |
| CSCsq78343 | Cisco IOS | Tidy up the netflow sub flow code |
| CSCsq96144 | Cisco IOS | Netflow v9 Exported Data issue in case of ECMP |
| CSCsr04916 | Cisco IOS | PBR dropped the packets after add set vrf vpn1 back to the route-map |
| CSCsr63098 | Cisco IOS | VRF-Aware Smart-Call Home requirement |
| CSCsr99518 | Cisco IOS | Granikos should not init rekey after recieving new outbound SA at QM3 |
| CSCsu11487 | Cisco IOS | pm_fec_is_mec() returns FALSE when 1 of 5 local MEC members is shutdown |
| CSCsu27660 | Cisco IOS | CDP packet sent tagged in internal vlan |
| CSCsu29301 | Cisco IOS | C2W21: Ingress SPAN on Sup - ACE module duplicates packets |
| CSCsu36715 | Cisco IOS | W2.0 : C2 : ION : Memory Leak in MSDP process |
| CSCsu67413 | Cisco IOS | RRI - Route disappears after ipsec rekey with multi int scenario |
| CSCsu92395 | Cisco IOS | Crash caused by event manager configuration: "action mail" |
| CSCsv12378 | Cisco IOS | c2w2:Memory leak in Crypto IKMP process on IOS EzVPN server |
| CSCsv24908 | Cisco IOS | L2 Fwd Broken on other modules when SIP-400 int flaps |
| CSCsv27372 | Cisco IOS | telnet to a real(directed mode) via GRE tunnel crates SUP crash on SRC2 |
| CSCsv27548 | Cisco IOS | Cat6k/sip200: PPP packets punted sip200 multilink interface |
| CSCsv27617 | Cisco IOS | Flow creation disabled in netflow table after reload for WAN main ints |
| CSCsv52025 | Cisco IOS | call-home: Port numbers cannot be added to URLs with IP addresses |
| CSCsv59334 | Cisco IOS | Connected nets redistr from eigrpTObgp when  no net 0 is set under eigrp |
| CSCsv63799 | Cisco IOS | PfR MC/BR bus error crash in ip fast flow |
| CSCsw14147 | Cisco IOS | VACL unable to capture traffic from RP |
| CSCsw32280 | Cisco IOS | Diag error on WS-X6148A-45AF card asic with Traffic |
| CSCsw41706 | Cisco IOS | router reload when registering EEM service diag script |
| CSCsw48181 | Cisco IOS | Unknown Unicast is dropped on Shut/no Shut of a VLAN |
| CSCsw52819 | Cisco IOS | Kernel dumper needs a few enhancements. |
| CSCsw68514 | Cisco IOS | SLB probes iin TESTing state while using client cmd in Vserver config |
| CSCsw76117 | Cisco IOS | TBs seen after redundancy mode change from sso to rpr |
| CSCsw78413 | Cisco IOS | BFD over ATM subinterfaces is broken in recent SR images |
| CSCsw83488 | Cisco IOS | Negative value seen for counters in vpn session |
| CSCsx09110 | Cisco IOS | Failed to establish ipsec tunnel with CCM |
| CSCsx20862 | Cisco IOS | Peer RP index unknown messages seen on VSS setup |

| Identifier | Technology | Description |
|---|---|---|
| CSCsx21886 | Cisco IOS | ISSU switchover command sync issue |
| CSCsx29377 | Cisco IOS | 1 sec multicast loss on standby sup720-10g |
| CSCsx49889 | Cisco IOS | SPA-IPSEC-2G-3-ACEI0TCAMFAILE:SpdSpInstall:cannot install Sp TmInsertSp |
| CSCsx55152 | Cisco IOS | Switch does not send TC trap if it is not a root bridge |
| CSCsx58786 | Cisco IOS | Router crash @ routemap_track_nexthop |
| CSCsx82825 | Cisco IOS | Shutdown Loopback interfaces in VSS recovery mode |
| CSCsy01275 | Cisco IOS | W15::  SYS-2-MALLOCFAIL: Memory allocation message seen after bootup |
| CSCsy01763 | Cisco IOS | 15 - 20 packets leek to DST with PACL after SSO |
| CSCsy03587 | Cisco IOS | c2w2b: SYS-2-MALLOCFAIL: Memory allocation  failed seen with tracebacks |
| CSCsy08838 | Cisco IOS | Zamboni allows clear packet inbound on protected interface |
| CSCsy16220 | Cisco IOS | a switch may crash due to deadlock between snmp and eem |
| CSCsy21797 | Cisco IOS | Cat6k-Unexpected SNMP messages occurred |
| CSCsy24895 | Cisco IOS | Memory leak in ACE HAPI process |
| CSCsy26526 | Cisco IOS | Router is getting crashed at netconf_sessionQs_set_max_message |
| CSCsy26979 | Cisco IOS | 33SXH5: Traceback seen @satvs_assert_class3 |
| CSCsy34566 | Cisco IOS | Disable VLAN mapping on ME6524, 6148A-GE-TX |
| CSCsy37175 | Cisco IOS | 2FE-PA Subintf lost connection after chassis/Flexwan2 reload |
| CSCsy41526 | Cisco IOS | PIM msgs duplicated when MPLS configured and IGMP Snooping Off on xface |
| CSCsy54365 | Cisco IOS | frequent datapath recovery and traffic loss on WS-X6704 with DFC |
| CSCsy58886 | Cisco IOS | NGN:Active crashes when standby booting up on SRC2->SRC3 ISSU |
| CSCsy61956 | Cisco IOS | Crash in ios-base when running 'show ip route' or 'show bgp' commands |
| CSCsy62753 | Cisco IOS | MST configured router crashed after receiving PVST BPDU. |
| CSCsy69228 | Cisco IOS | Add CLI mls cef tunnel fragment support for non supertycho2 |
| CSCsy69740 | Cisco IOS | SXH: Traffic drop on L2 PO after cleared psecurity on rcving L2 ports |
| CSCsy78994 | Cisco IOS | Memory leak in Service Task |
| CSCsy82121 | Cisco IOS | IGMP Source only not working due to MC_CAP not set |
| CSCsy85171 | Cisco IOS | CDL2 Read Error: Time out |
| CSCsy86050 | Cisco IOS | MAC Move Notifications on VSS between active and down ports |
| CSCsy87619 | Cisco IOS | VSS port channel going down when powering down active switch |
| CSCsy95520 | Cisco IOS | ~500msec Pkt loss after transition to HSRP Active on L3 int |
| CSCsz01976 | Cisco IOS | Need a cli to dump the rommon environment and unset rommon variable |
| CSCsz06187 | Cisco IOS | VACL capture for ingress software switched packets |
| CSCsz07068 | Cisco IOS | VSS: Output Drops on a VSL port due to small Tx Queue limit |
| CSCsz12369 | Cisco IOS | FPD support for SPA-8X1FE-TX-V2 is not enabled |
| CSCsz14072 | Cisco IOS | Memory leak at "MAB Framework" process when dot1x is enabled |
| CSCsz20625 | Cisco IOS | Error message seen if SIP Is OIR'd during Standby SUP bootup |
| CSCsz22954 | Cisco IOS | Supported  WS-X6324-100FX-MM is powered down improperly |

| Identifier | Technology | Description |
|---|---|---|
| CSCsz23448 | Cisco IOS | SIP 200 not coming up and Router Crashes after applying card type E3 1 1 |
| CSCsz40969 | Cisco IOS | Need to add Me_Kr flow-control status registers back into sierra/whitney |
| CSCsz42143 | Cisco IOS | WS-X6148A-GE-TX  module fails keepalives when excessive errors on port. |
| CSCsz44678 | Cisco IOS | Tunnel won't forward traffic across global to vrf |
| CSCsz47077 | Cisco IOS | SWITCH_NUMBER rommon variable set on its own and by "wr erase" command |
| CSCsz55834 | Cisco IOS | GLBP may provided BIA MAC instead of Virtual MAC for mobile users |
| CSCsz62046 | Cisco IOS | Crash at memcpy after CPUHOG in SNMP ENGINE |
| CSCsz63359 | Cisco IOS | c2w2b:"show mls qos ip" displays vslot interface instead switchid and sl |
| CSCsz67334 | Cisco IOS | ciscoEnvMonTemperatureStatus trap sent sporadically as NotFunctioning |
| CSCsz71970 | Cisco IOS | c2w2b: Freed Memory being Accessed by lldp_med_free_local_annex |
| CSCsz75820 | Cisco IOS | JQL: VSS hang on SP after RP crashed by software-forced reload |
| CSCsz76015 | Cisco IOS | C2W2: Need cli to set PF_BIAS to ensure lower slot# Sup boots as active |
| CSCsz84544 | Cisco IOS | output drops increment on not-connected interface of 6548GE-TX module |
| CSCsz87648 | Cisco IOS | SP/RP and redundant system handshake broken when the kernel crashes. |
| CSCsz92508 | Cisco IOS | SPA module reloads when no response to keep-alive polling |
| CSCta01121 | Cisco IOS | c2w1:MDEBUG traceback is seen while unconfiguring qos feature in FM. |
| CSCta05502 | Cisco IOS | Spurious memory access made at psecure_port_del_addr_by_mac_imp |
| CSCta06175 | Cisco IOS | Cat6500/SXH: Deleted configs re-appear on IDSM reset |
| CSCta10870 | Cisco IOS | FPOE takes long time to be programmed on active vss switch |
| CSCta21771 | Cisco IOS | %CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at  0 error on modul |
| CSCta27279 | Cisco IOS | WCCP s/w switching with Ingress redirection & interface ACL |
| CSCta48968 | Cisco IOS | Modular IOS kernel crashinfo has missing information |
| CSCta52689 | Cisco IOS | cat6k crash in RP due to address error with wccp configuration |
| CSCta53157 | Cisco IOS | SPA-4XT3/E3 int in SIP-200 admin-down on standby after fpd upgrade |
| CSCta55498 | Cisco IOS | [Modular IOS] MIPS CP0 registers save algorthim needs a few improvements |
| CSCta74315 | Cisco IOS | WS-X6324-100FX-MM May Be Inoperable and Have Status "Other" |
| CSCta76808 | Cisco IOS | add CLI command for medium buffer pool |
| CSCta94179 | Cisco IOS | Recirculated MPLS packets becasue of egress service policy are dropped |
| CSCtb23289 | Cisco IOS | Major temperature alarm has to force system shutdown |
| CSCtb28032 | Cisco IOS | Changing module corrupts Flex Link |
| CSCtb28712 | Cisco IOS | SPAN Reflector not enabled for WS-SVC-ADM-1-K9 |
| CSCtb38547 | Cisco IOS | Incorrect CP0 values and empty kernel variable section in kernel crashin |
| CSCtb60330 | Cisco IOS | VTI: Missed DPD ACK on phase 1 expiry causing phase 2 deletion. |
| CSCtb63352 | Cisco IOS | VSS: With 6KW DC PS, no power to bringup VSL supervisor or linecard |
| CSCtb66983 | Cisco IOS | Nas-port-type is missing in Access-request |
| CSCtb68478 | Cisco IOS | "Illegal nextSsIndex value" message should be removed |
| CSCtb87454 | Cisco IOS | DHCP Rogue Server Detection |

| Identifier | Technology | Description |
|---|---|---|
| CSCee83031 | Infrastructure | test crash, dumping log before command is displayed |
| CSCsc77704 | Infrastructure | region_find_by_addr goes into infinite loop when spurious memory occurs. |
| CSCsc88003 | Infrastructure | Issuing banner exec commnad under interface range crash switch |
| CSCsd99763 | Infrastructure | Cisco 7200 series reload unexpectedly while configuring BGP acces list |
| CSCse40379 | Infrastructure | IP SLA: Increasing the request-data-size via CLI crashes the device. |
| CSCsk41686 | Infrastructure | PARSER-3-CFGLOG_NOMEM: constanlty in log |
| CSCsm66896 | Infrastructure | IP SLA Monitor strDupOctet memory leak |
| CSCsq74185 | Infrastructure | Image verification not possible on 12.2(33)SRC for the c7200 |
| CSCsr08750 | Infrastructure | router is crashing after giving the command memory reserve critical 1 |
| CSCsr94474 | Infrastructure | Running-config stuck: nv_csb_semaphore locked during copy run ftp |
| CSCsu65967 | Infrastructure | Modular IOS crash at free_lite_internal |
| CSCsv90106 | Infrastructure | nested crash leads to incomplete crashinfo |
| CSCsx10028 | Infrastructure | Core dump may fail to write |
| CSCsy86078 | Infrastructure | Memory corruption Failure |
| CSCsz19466 | Infrastructure | C2W1: int range command with port-channel load-defer cause router crash |
| CSCsz52815 | Infrastructure | Crash when 'history hours-of-statistics-kept' has value greater than 9 |
| CSCta02715 | Infrastructure | SXH5: RP crash on each booting time if <logging count> enabled |
| CSCed01880 | IPServices | Not able to configure NAT tcp timeouts beyond 4194 sec |
| CSCsa41736 | IPServices | Router crash after enable NAT rate-limit feature |
| CSCsa47672 | IPServices | NAT refcount counter maximum value of 65536 (64K) |
| CSCse01431 | IPServices | NAT-CCE : NAT SBC : outside sip call not go through |
| CSCse66643 | IPServices | SYS-2-NOBLOCK error when redistributing NAT routes |
| CSCsj19805 | IPServices | ip igmp static-group broken after reload on int vlan on a 7600 |
| CSCsk23972 | IPServices | Telnet failed with "No wild listener" error |
| CSCsw52416 | IPServices | NAT: dynamic nat entries do not timeout in certain case |
| CSCsw65614 | IPServices | NAT with route maps doesn't work for TCP application |
| CSCsx33622 | IPServices | Fix MSS calcuation issue in TCP |
| CSCsx34372 | IPServices | c2w21/C2W2b:OSPF is not working with udlr/ude |
| CSCsy39623 | IPServices | cannot ping local vlan interface ip address with NAT configured |
| CSCsy39667 | IPServices | dhcp-proxy-client incorrectly sends DHCPRELEASE in PPP-agg use-case |
| CSCsy97506 | IPServices | All nat'ed multicast packets punted to software |
| CSCsz12488 | IPServices | LDAP add with malformed BER attributes causes CPUHOG and MALLOCFAIL |
| CSCsz56393 | IPServices | Modular IOS - SUP720 - Sends malformed syslog packet |
| CSCsz89107 | IPServices | high cpu due to ip_input process during SNMP trap |
| CSCsz91851 | IPServices | NAT : ESP packets not translated with static NAT outside translation |
| CSCta24043 | IPServices | "%IPNAT-4-ADDR_ALLOC_FAIL" message seen when all ports are not allocated |
| CSCta83548 | IPServices | NAT Platform: unable to clear an specific nat entry |

| Identifier | Technology | Description |
|---|---|---|
| CSCta89283 | IPServices | Add support for NAT redundancy feature in SX releases |
| CSCtb58282 | IPServices | show tcp brief can cause crash |
| CSCsz71787 | LegacyProtocols | Router crash by crafted IP packet. |
| CSCej82248 | MPLS | %LFD-3-NOOCE: Traceback in lfd_fib_update_mpls_oces |
| CSCsy60668 | MPLS | W1.5:: Toggle "mpls tra router-id" cause router crash |
| CSCsz11877 | MPLS | MPLS-TE Tunnel label re-allocation on mid-point router while RSVP-GR |
| CSCsz75180 | MPLS | Crash due to mpls subintf being removed |
| CSCsz92368 | MPLS | MDEBUG-2-ACCESSFREED: @tc_handle_dead_peers Enabling/disabling "mpls ip" |
| CSCsx34506 | Multicast | RPF failure with no PIM neighbor triggers PIM Hello |
| CSCta26106 | QoS | RSVP-3-CONSISTENCY error followed by an unexpected reboot. |
| CSCse15634 | Routing | neighbor default-originate doesn't work in address-family ipv4 multicast |
| CSCse45978 | Routing | BGP to RIP redistribution breaks as RIP nexthop moves to alternate path |
| CSCsg92473 | Routing | Switch crashes - IPV6 reflexive acl scalability test |
| CSCsl90028 | Routing | CEF low mem crash after pumping more than 1Lac OSPF routes |
| CSCsm05082 | Routing | BGP Dampening penalty not decaying on frqnt 'sh ip bgp v all' [dampening |
| CSCsm79085 | Routing | EIGRP routes flapping due to nexthop changed |
| CSCso07371 | Routing | SCHED-7-WATCH: Attempt to set uninitialized watched boolean in pfxlist |
| CSCsq20928 | Routing | CEFv6 dropping IPv6 unicast packets |
| CSCsq45082 | Routing | ip route with associated track/sla gets removed when track is still up |
| CSCsq83006 | Routing | Port-channel down makes EIGRP SIA |
| CSCsr27794 | Routing | BGP updates stuck during peer flap |
| CSCsu96698 | Routing | BGP: /32 route being advertised while 'summary-only' is configured |
| CSCsv17933 | Routing | Static route in VRF is not redistributed by RIP after link flap |
| CSCsv73754 | Routing | crash during vrf unconfig - bgp_vpn_impq_add_vrfs_cfg_changes |
| CSCsx08294 | Routing | OSPF encounters a bus error crash when running SPF |
| CSCsx51299 | Routing | Crash when remove and configure ipv6 ACL via telnet and console |
| CSCsx98673 | Routing | PE not send extended-community to a peer newly added to peer-group |
| CSCsy29534 | Routing | Bus error crash on removing address-familly in router rip config mode |
| CSCsy73123 | Routing | Connected route on port-channel subintf not removed when Po is down |
| CSCsy76404 | Routing | Modular IOS: memory leak in CEF background process |
| CSCsy77842 | Routing | TB isis_process_no_router after isis router process deleted |
| CSCsy84134 | Routing | ARP table is flushed when deleting secondary IP address |
| CSCsz16724 | Routing | BGPv6: default-metric is not being NVGEN'ed and not functionting |
| CSCta60119 | Routing | non recursive accounting can cause prefixes linked to drop |
| CSCsc49862 | Security | IPaddress in Subject Alternative Name is not parsed correctly. |
| CSCso27236 | Security | IOS CA client shows renew date 1 Jan 1970 |
| CSCsv23797 | Security | SSH:Crash seen on 7200 on mcp_dev |

| Identifier | Technology | Description |
|---|---|---|
| CSCsv54863 | Security | IOS PKI: Not expired Certificate is deleted if autoenrollment fails |
| CSCsz84055 | Security | System crashed unexpected while open ssh2 session |
| CSCtb36521 | Security | PKI get stuck in pager when requesting to fetch SCEP capabilites |
| CSCtc41114 | Security | New SSH sessions with RSA key fails after changing hostname |
| CSCsi56413 | WAN | PA-POS-OC3SMI interface output stuck . |

## Caveats Resolved in Release 12.2(33)SXH5

### Resolved AAA Caveats

- CSCsv73509—Resolved in 12.2(33)SXH5

  **Symptoms:** When "no aaa new-model" is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

  **Conditions:** Configure "no aaa new-model", configure **login local** under **line vty 0 4** and configure **login tacacs** under **line vty 0 4**.

  **Workaround:** There is no workaround.

### Resolved Infrastructure Caveats

- CSCsr72301—Resolved in 12.2(33)SXH5

  **Symptom:** Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http

  **Conditions:** See "Additional Information" section in the posted response for further details.

  **Workarounds:** See "Workaround" section in the posted response for further details.

- CSCsx49573—Resolved in 12.2(33)SXH5

  **Symptom:** Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http

  **Conditions:** See "Additional Information" section in the posted response for further details.

  **Workarounds:** See "Workaround" section in the posted response for further details.

### Resolved IPServices Caveats

- CSCsk64158—Resolved in 12.2(33)SXH5

  Several features within Cisco IOS Software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory.

This advisory is posted at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

- CSCsm27071—Resolved in 12.2(33)SXH5

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS Software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  – The configured feature may stop accepting new connections or sessions.
  – The memory of the device may be consumed.
  – The device may experience prolonged high CPU utilization.
  – The device may reload.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory.

  The advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- CSCsm45390—Resolved in 12.2(33)SXH5

  **Symptom:** An IOS software crash may occur when receiving a specific malformed DHCP packet.

  **Conditions:** An IOS device configured for DHCP Server and receives a DHCP-request from a DHCP relay device. A specific malformed option in the packet packet may induce a software traceback or crash. The specific packet will not occur without manual modification.

  **Workaround:** None.

- CSCsv04836—Resolved in 12.2(33)SXH5

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24.

- CSCsw18636—Resolved in 12.2(33)SXH5

  **Symptom:** High CPU utilization after receives a ARP packet with protocol type as 0x1000.

  **Conditions:** This problem occurs on SUP32 running 12.2(33)SXI. This problem does not occur on SUP720. The problem is only seen when you have bridge-group CLI being used which lead to arp pkts with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

**Workaround:** Filter the ARP packet. The device Config should have bridge-group creation first; followed by interface specific bridge-group options.

**Additional Information:** This problem is now isolated to command ordering in the startup-config file. The **bridge <>** command is saved before the **bridge-group <>** command (which is run in the interface-config mode) is saved. The linking of IDB to bridge structure is not happening correctly and some check fails in the bridge code that lets the packet to be processed again and again instead of being dropped.

If the **bridge-group <>** command is removed in the startup-config and only applied after the **bridge <>** command is run, the problem will go away. Please use this workaround until a fix is put in.

- CSCsr29468—Resolved in 12.2(33)SXH5

  Cisco IOS Software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

#### Resolved LAN Caveats

- CSCsv05934—Resolved in 12.2(33)SXH5

  **Summary:** Cisco's VTP protocol implementation in some versions of Cisco IOS and CatOS may be vulnerable to a DoS attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash (and reload/hang). The crafted packet must be received on a switch interface configured to operate as a trunk port.

  **Workarounds:** There are no workarounds available for this vulnerability.

  This response is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20081105-vtp

#### Resolved Multicast Caveats

- CSCso90058—Resolved in 12.2(33)SXH5

  **Symptom:** MSFC crashes with RedZone memory corruption.

  **Conditions:** This problem is seen when processing an Auto-RP packet and NAT is enabled.

  **Workaround:** None known at this time.

- CSCsu79754—Resolved in 12.2(33)SXH5

  **Symptoms:** PIM packets may be processed on interfaces which PIM is not explicitly configured.

  **Conditions:** Unknown at this time.

  **Workarounds:** Create an ACL to drop PIM packets to such interfaces.

### Resolved Routing Caveats

- CSCsx73770—Resolved in 12.2(33)SXH5

  **Symptom:** A Cisco IOS device that receives a BGP update message and as a result of AS prepending needs to send an update downstream that would have over 255 AS hops will send an invalid formatted update. This update when received by a downstream BGP speaker triggers a NOTIFICATION back to the sender which results in the BGP session being reset.

  **Conditions:** This problem is seen when a Cisco IOS device receives a BGP update and due to a combination of either inbound, outbound, or both AS prepending it needs to send an update downstream that has more than 255 AS hops.

  **Workaround:** The workaround is to implement **bgp maxas-limit X** on the device that after prepending would need to send an update with over 255 AS hops. Since IOS limits the route-map prepending value to 10 the most that could be added is 21 AS hops (10 on ingress, 10 on egress, and 1 for normal eBGP AS hop addition). Therefore, a conservative value to configure would be 200 to prevent this condition.

### Other Resolved Caveats in Release 12.2(33)SXH5

| Identifier | Technology | Description |
|---|---|---|
| CSCec82106 | AAA | Router crashes with a bus error when removing AAA comands |
| CSCei62358 | AAA | Downloading callback-dialstring as part of Tacacs+ author leads to crash |
| CSCin40015 | AAA | telnet to NAS fails when user profile has access-profile |
| CSCsc78999 | AAA | Address Error exception at TPLUS |
| CSCse02550 | AAA | ip radius source-interface not used in combination with vrf |
| CSCsl63494 | AAA | Issue with session accounting in AAA |
| CSCsq37815 | AAA | Case sensitive Username authentication is passed with wrong user name |
| CSCsq94524 | AAA | "aaa accounting update newinfo" causes extra "jitter maximum 0" option |
| CSCsv06973 | AAA | Router Crashes at tplus_shutdown_single_connection |
| CSCsw19816 | AAA | cat6000: IOS login enhancments not creating logs for telnet with AAA |
| CSCsy00716 | AAA | Accounting record has sensitive information in clear text structure |
| CSCso64050 | ATM | HA functionality is not working when policy attached to atm pvc |
| CSCeg35237 | Cisco IOS | Watchdog crash after sh crypto session |
| CSCeg80842 | Cisco IOS | PA-MC-8TE1 controller stuck ( similar to CSCdz72292 ) |
| CSCek70131 | Cisco IOS | SIP1 crash at vip_mlp_fastsend with HEARTBEAT error for mlppp qos |
| CSCek77996 | Cisco IOS | High CPU caused by data traffic with crypto map in crypto connect mode |
| CSCsd04608 | Cisco IOS | MQC-IPHC: Router crashed while testing mqc-iphc test |
| CSCsd45698 | Cisco IOS | Cat6K: SLB punted to CPU if src_index is port-channel index |
| CSCse63833 | Cisco IOS | SNMP bus error while polling cipsStaticCryptomapTable . |
| CSCsg14926 | Cisco IOS | Standby can not boot because of insufficient memory with 32K interfaces |
| CSCsg83756 | Cisco IOS | SPA-8XCHT1/E1 after Reload C/A LED green even if no cable plugged |
| CSCsg87290 | Cisco IOS | SIP1-ChOC3: Extra path flap is observed on ChOC3 SPA interfaces |
| CSCsh22225 | Cisco IOS | CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR: |
| CSCsi55428 | Cisco IOS | FRU Trap sequence incorrect when " hw-module subslot shutdown unpowered" |

| Identifier | Technology | Description |
|---|---|---|
| CSCsi78584 | Cisco IOS | T3/E3 SPA:Line protocol is not comin up with E3 and framing bypass |
| CSCsj19308 | Cisco IOS | PE and CE ping fails over multilink ppp bundle. . |
| CSCsk30196 | Cisco IOS | BADBUFFER error at pak_copy_contiguous_to_contiguous |
| CSCsk33045 | Cisco IOS | MST BPDU *must* be sent untagged, even when the switch is configured wit |
| CSCsk49151 | Cisco IOS | Vlan policy-map rejected upon reloading. |
| CSCsk67417 | Cisco IOS | Crash while two or more users displays: show ip arp inspection log |
| CSCsk84498 | Cisco IOS | EVERGLADES:archive,write-mem feature broken |
| CSCsk89091 | Cisco IOS | HWIF-QOS-ERR: Failure installing Port QoS TX/Rx setting |
| CSCsl44170 | Cisco IOS | LI tapped PPPoE LCP/PPP control packets originated from router are bogus |
| CSCsl53279 | Cisco IOS | Physical interfaces on Cat6k set to 10 usec regardless of line speed |
| CSCsl72332 | Cisco IOS | cat6k crash with 'no mobility network-id 4' |
| CSCsm44147 | Cisco IOS | SSO failure due to mismatched command on SRB1 |
| CSCsm66678 | Cisco IOS | Policing not working in MPLS cloud |
| CSCsm72121 | Cisco IOS | W2: bad cookie magic was detected after SSO switchover with sh vtp count |
| CSCsm74948 | Cisco IOS | mVPN RP does not send join to directed connected neigbor PE |
| CSCsm76792 | Cisco IOS | PM HA bulk sync posting RF_DONE before bulk sync has finished |
| CSCsm79995 | Cisco IOS | Tracebacks are seen while attaching service-policy in a atm  pvc |
| CSCsm83256 | Cisco IOS | IDSM2 Data port operation status not OK after boot OR SSO |
| CSCsm98671 | Cisco IOS | TestTrafficStress fails with certain configuration |
| CSCso03419 | Cisco IOS | VRF_Lite aware PBR: Set ip vrf clause changes on Reload/SSO with SIERRA. |
| CSCso05889 | Cisco IOS | Pak Subblock creation fails from CEF in ION |
| CSCso11489 | Cisco IOS | %SYS-SP-3-INVMEMINT while collecting ION crashinfo |
| CSCso11822 | Cisco IOS | LACP PC switchport, on OIR, "channel group 112 active" config gets lost |
| CSCso35659 | Cisco IOS | L3 traffic rate limited after adding and removing Xcon to a SVI |
| CSCso38671 | Cisco IOS | VS specific message seen on Sup32 image when "erase startup-config" |
| CSCso40891 | Cisco IOS | Stb rp reloaded during every bootup, process = FM, fm_free_platform_data |
| CSCso72250 | Cisco IOS | Incorrect color for SYSTEM led of Active and Standby sup in VS mode |
| CSCso88183 | Cisco IOS | DOME:dumper.proc crashes on dome when another process crashes |
| CSCso93350 | Cisco IOS | Boot string fails to set in rommon but no error message |
| CSCsq22383 | Cisco IOS | SP crash due to CPU hog by online diags |
| CSCsq56941 | Cisco IOS | 6500 - Static MAC cleared from port-channel member ints after reload |
| CSCsq73122 | Cisco IOS | Proxy-ARP returns BIA instead of VMAC with LAM |
| CSCsq82865 | Cisco IOS | Parsing error reading route-map match statements if longer than 254 chrs |
| CSCsq87496 | Cisco IOS | "%OIR-6-INSCARD" syslog not being send from the device |
| CSCsr06037 | Cisco IOS | the monitor session source is removed by deleting sub-interface |
| CSCsr08482 | Cisco IOS | PM support to program ethertype to all ports when port-group in mux mode |
| CSCsr09062 | Cisco IOS | MLP+QoS - Memory corruption due to Change BW and flap int |

| Identifier | Technology | Description |
|---|---|---|
| CSCsr24647 | Cisco IOS | MSFC autostate don't up svclc Vlan int after two SSO switchover |
| CSCsr29559 | Cisco IOS | WCCP flap corrupts mcast CEF adjacency |
| CSCsr39272 | Cisco IOS | %DATACORRUPTION-1 due to spa sensor temp overruning buffer |
| CSCsr88845 | Cisco IOS | unicast BootP replies dropped by DHCP snooping |
| CSCsu01372 | Cisco IOS | 33SB: Result of boot config command not sync to standby RP after reload |
| CSCsu10022 | Cisco IOS | L2 traffic is policed when CoPP is enabled |
| CSCsu33707 | Cisco IOS | Multicast traffic will not stop after PIM prune |
| CSCsu40077 | Cisco IOS | MAB + Dot1x + aggressive timers leave port unauthorized but forwarding |
| CSCsu40166 | Cisco IOS | PBR packets send out to wrong next hop MAC after ACL is changed |
| CSCsu48241 | Cisco IOS | memory leak when removing igmp snooping with acl filtering |
| CSCsu49257 | Cisco IOS | Cstn-id timer should be restarted when access-request is seen |
| CSCsu50413 | Cisco IOS | RE: acl merge causes high rp cpu for ~50 min after reload |
| CSCsu67559 | Cisco IOS | Copy Run Start does not provide the same functionality as 'wr mem' |
| CSCsu75546 | Cisco IOS | C2W21: traffic not span to NAM using span conf mode local-tx source intf |
| CSCsu81158 | Cisco IOS | Pkt drops on SIP-400 LC due to QoS lock fail for subintfs. |
| CSCsu83563 | Cisco IOS | MMLS:If rate-lt on when STDBY reloads, doesnt work on swovr:x40/dual RSP |
| CSCsu86524 | Cisco IOS | IKMP process leak: check_ipsec_proposal |
| CSCsu88557 | Cisco IOS | [no] mdix auto" CLI command not present for WS-X6196-RJ21" |
| CSCsu91725 | Cisco IOS | Bus crash problem due to cipSecGlobalStats MIB query |
| CSCsu95237 | Cisco IOS | SSO switchover,clear packet seen on the wire exposing the inner IP pkt |
| CSCsu97020 | Cisco IOS | policer on flexwan/multilink is dropping even CIR is not reached |
| CSCsu99270 | Cisco IOS | CPUHOG observed when configuring more vlan interfaces |
| CSCsv05263 | Cisco IOS | Sup32 crashes when dumping r2d2 registers |
| CSCsv07858 | Cisco IOS | IfIndex for unconfigured VLAN on 7613 |
| CSCsv09249 | Cisco IOS | VSS after dual-active recovery MEC on standby chassis UDLD error disable |
| CSCsv14886 | Cisco IOS | Failure to send RADIUS state attribute |
| CSCsv17989 | Cisco IOS | interface in SIP200 show "admin down" when it is physical down |
| CSCsv20339 | Cisco IOS | MN history table is flooded with multiple (~500) add/delete entries |
| CSCsv20768 | Cisco IOS | After SSO s/wover, atm clock config changes to line and PTB to UNSTABLE |
| CSCsv20920 | Cisco IOS | telnet from a GRE tunnel to real address for DNS vserver fails |
| CSCsv22779 | Cisco IOS | VRF-PBR: Packets dropped with reflexive acl |
| CSCsv24742 | Cisco IOS | PfR exit link is OOP when interface counter wraps |
| CSCsv30679 | Cisco IOS | Sup detetes Vlans from Sup IDSM Config on startup / failover |
| CSCsv32101 | Cisco IOS | QoS: memory corruption traceback when using access-list with time range |
| CSCsv37543 | Cisco IOS | GRE/IPsec misconfig is only resovled through module or chassis reload |
| CSCsv38928 | Cisco IOS | IGMP Snooping does not send out Global query on 2nd TCN < 35 seconds |
| CSCsv43991 | Cisco IOS | FWSM's internal portchannel on the cat6k side goes down after upgrading |

| Identifier | Technology | Description |
|---|---|---|
| CSCsv44923 | Cisco IOS | MAC move behind phone leads to lost connectivity with MAB |
| CSCsv52426 | Cisco IOS | GRE Recirc index is 0x0 in adjacency hence encap operation fails on DFC |
| CSCsv57235 | Cisco IOS | duplex is changing automatically on WS-X6148-RJ-45 |
| CSCsv57305 | Cisco IOS | VSS: software forced reload with 100Mbps SFPs in supervisor uplink ports |
| CSCsv58279 | Cisco IOS | Reload due to Address Error with multicast configuration |
| CSCsv60643 | Cisco IOS | sup4 when toggled 10g mode the config is not synced to standby sup |
| CSCsv64079 | Cisco IOS | SXF7: Patching fails with WiSM Card on Cat6500 |
| CSCsv66706 | Cisco IOS | IDSM port-channel Allowed-Vlan statements lost on reload |
| CSCsv66827 | Cisco IOS | Clearing the SSH session from a different vty session crashes the box. |
| CSCsv73299 | Cisco IOS | L2 multicast forwarding broken with DHCP snooping & TTL rate-limiter |
| CSCsv74607 | Cisco IOS | Pid 21: Process "IPC Seat Manager" stack 0x4732A474 savedsp 0x5002AE98 |
| CSCsv75511 | Cisco IOS | VSS:NAM on standby switch can't reach netwk after unconfig re-config ... |
| CSCsv76509 | Cisco IOS | Cat6k/MSTP in compat mode BPDUs sent in VLAN1 regardless of config |
| CSCsv85551 | Cisco IOS | SP crash due to consume all scp triggered by OIR loop when PS go off |
| CSCsv86288 | Cisco IOS | Sending a hello response with a session-id element causes a crash |
| CSCsv92872 | Cisco IOS | 10GE link on Sup720-10GE takes more than 30sec to go down during crash |
| CSCsw17478 | Cisco IOS | PVT HOSTS- ports programmed with incorrect rdt index upon bootup |
| CSCsw18793 | Cisco IOS | VRF-PBR: TCAM adjacency not programmed with multiset policy order after |
| CSCsw25255 | Cisco IOS | Rapid PVST : Slow convergence unless debug spanning event is turned on |
| CSCsw31607 | Cisco IOS | LTL index incorrect in PI MET table |
| CSCsw39798 | Cisco IOS | Sup32 failover causes line protocol down to IP phone with dot1x config |
| CSCsw41168 | Cisco IOS | %ALIGN-3-SPURIOUS at sm_get_portEntPhyIndex |
| CSCsw41439 | Cisco IOS | W21,VSL,SNMP,cvsCoreSwitchPreempt,cvsCoreSwitchPriority not SSO aware. |
| CSCsw43953 | Cisco IOS | Card not identified SIP Is OIR'd during Standby SUP bootup |
| CSCsw45396 | Cisco IOS | when STP recovered in uplinkfast,no sent dummy multicast packets |
| CSCsw48824 | Cisco IOS | Switchport Block Unicast - prevents RTP on same VLAN |
| CSCsw51395 | Cisco IOS | Proper handling is required for Mac-Filter with Port-security |
| CSCsw53362 | Cisco IOS | c2w2b: Device crashes with NAT stress test |
| CSCsw59517 | Cisco IOS | IGMPv3 snooping drops 'Block Old Sources' report |
| CSCsw73302 | Cisco IOS | memory leak in qm_increment_ag_policer_usage on standby-rp |
| CSCsw82732 | Cisco IOS | VPN-SPA internal vlan interface wedged in SXH4 |
| CSCsw87352 | Cisco IOS | 6748's port can not forwarding traffic - port src index wrong |
| CSCsw87563 | Cisco IOS | packets with multicast mac and unicast ip are software routed by cat6500 |
| CSCsw90798 | Cisco IOS | Bus error crash after configuring vlan name change |
| CSCsw98231 | Cisco IOS | SDBY stuck @ CEF RRP RF Client(5025) after ISSU RV |
| CSCsx16206 | Cisco IOS | Traffic loss issue from SFM capable modules to other device through DEC |
| CSCsx37615 | Cisco IOS | VSS: rem comm standby-rp sh plat hardware capacity may reset switch |

| Identifier | Technology | Description |
|---|---|---|
| CSCsx39263 | Cisco IOS | TCAM entries are not installed for TCP intercept after SSO |
| CSCsx70229 | Cisco IOS | Add the symbols back in SXH throttle which were removed by CSCsw82732 |
| CSCsx76308 | Cisco IOS | HA client crashing attempting to free unassigned memory |
| CSCsx83443 | Cisco IOS | crypto debug condition leaks messages which lead to high cpu. |
| CSCsy22802 | Cisco IOS | MPLS VPN broken, vrf connection (permit missing for internal vlan acl) |
| CSCsy24691 | Cisco IOS | entPhysicalTable has power-input 3 Sensor for 6kW DC PS1 and not PS2 |
| CSCsy79691 | Cisco IOS | RP crash with dot1x critical authentication configured |
| CSCsy83830 | Cisco IOS | IOS-RLB crashes while deleting the username sticky |
| CSCsy96102 | Cisco IOS | FM-4-MPLS_RSVD_VLAN_ERROR-failed to remove feature when vrf delete |
| CSCsr27727 | Content | Cat6K experiences a reload after %SYS-2-ASSERTION_FAILED: message |
| CSCsx40747 | Content | Router hangs while doing ip casa configurations |
| CSCed33145 | Infrastructure | line vty exec-timeout not working properly, def causes spur mem acc |
| CSCef82896 | Infrastructure | When removing the user name from auth dialog, http crashes |
| CSCek62770 | Infrastructure | bundles need to include CW_ strings |
| CSCin79116 | Infrastructure | show memory summary could push the CPU util to 100% |
| CSCsb98906 | Infrastructure | Memory Leak with bgp regexp deterministic configuration |
| CSCsc86307 | Infrastructure | c3845 crashed @ show_systat |
| CSCsd55059 | Infrastructure | polling CISCO-FLASH-MIB slows down GSR |
| CSCse41523 | Infrastructure | bootldr config caused stbyPRE reset if file does not exist on stby-bootf |
| CSCse49151 | Infrastructure | 3800 clock slip over times verified in lab |
| CSCsh66245 | Infrastructure | Lowest memory is too low after reload on Cisco 10000 |
| CSCsj24186 | Infrastructure | %SYS-2-NOBLOCK messages from Pool Manager process |
| CSCsj67434 | Infrastructure | The CLI: 'parser config cache interface' does not work |
| CSCsm27493 | Infrastructure | procmib_server port has to send rpc reply only for RPC requests. |
| CSCso29361 | Infrastructure | cfg added under interface range vlan not being added in redundant sup |
| CSCsq19159 | Infrastructure | RP crashes in chassismib_add_sub_card_entry after linecard reload |
| CSCsv80900 | Infrastructure | W21:: EARL-SPSTBY-2-SWITCH_BUS_IDLE & PF_ASIC-SPSTBY-3-ASIC_DUMP @boot |
| CSCsv86766 | Infrastructure | Signature fail while copy, causing system:/running-config to be deleted |
| CSCsw35917 | Infrastructure | SP syslog messages not sent as SNMP traps by RP's SNMP agent |
| CSCsw61555 | Infrastructure | Router Crashes after doing SSO |
| CSCsx32841 | Infrastructure | ceImageDescription may exceed 255 characters |
| CSCsx95675 | Infrastructure | interface config disappear after "wr mem" |
| CSCsy55455 | Infrastructure | Crash at saaComponentGet |
| CSCec72958 | IPServices | Software forced crash when translating LDAP packet |
| CSCef58137 | IPServices | Router Crash after high CPU, when IPNAT configured with route-map |
| CSCek10384 | IPServices | 7200 NAT dropping Out to In ESP Packets |
| CSCsh49973 | IPServices | NAT-ALG corrupts offset value of DNS PTR response |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj41479 | IPServices | DHCP Services should not be enabled by default in IOS |
| CSCsj76907 | IPServices | IPv6 UDP sockets may incorrectly show "--any--" for local address |
| CSCsk16821 | IPServices | DHCP does not NAK after DHCPREQUEST from unknown client . |
| CSCsm89795 | IPServices | Orbitty repeatedly Crashes - Succeptible to Denial of service attacks |
| CSCso02053 | IPServices | NAT does not add dynamic aliases after reload. |
| CSCso04657 | IPServices | SSLVPN service stops accepting any new SSLVPN connections |
| CSCso39062 | IPServices | C2W2: %SYS-3-INVMEMINT: Invalid memory action message & TB's with PAT. |
| CSCso54027 | IPServices | Spurious memory access in ttcp_rcv_stats |
| CSCsq14311 | IPServices | 7200 crash - ipnat_unlock_parent_entry (PPTP) |
| CSCsq81365 | IPServices | MFI: UDP forwarded-protocols from VRF are leaked into global table |
| CSCsq92440 | IPServices | Router Crash with igmp static grp classmap for 10k grps on 10 subints |
| CSCsu10108 | IPServices | TFTP Server function is not working in 7600 router |
| CSCsu64215 | IPServices | ip tcp adjust-mss command results in packet loss for non-TCP traffic |
| CSCsu72176 | IPServices | Crash:Process Deadlock in Standby while reloading UUT with DHCP configs |
| CSCsu95319 | IPServices | IGMP report was not sent to helper address. |
| CSCsv16987 | IPServices | nat pool size more than 16 bit long should not be configured |
| CSCsv86201 | IPServices | Modular IOS : max sockets overflow |
| CSCsw16698 | IPServices | DHCP database could not be locked DHCPD process could not lock semaphore |
| CSCsw51864 | IPServices | CHUNKFREE error and crash when changing NAT config |
| CSCsw68135 | IPServices | Removing static nat with route-map cause Address Error |
| CSCsw73391 | IPServices | ip igmp limit gets stuck |
| CSCsx09343 | IPServices | Name resolution triggers pager in non-interactive mode. |
| CSCsx23602 | IPServices | crash after 'clear ip nat trans *' |
| CSCsx32283 | IPServices | Malformed L field in LDAP crashes 6k with NAT |
| CSCsx74657 | IPServices | Many issues with NAT/Multicast feature |
| CSCsy26750 | IPServices | 6k Crash with ipnat_ldap_fixup (Redundancy Checks needed) |
| CSCsy45371 | IPServices | NAT: two static nat entry related issues |
| CSCsw81485 | LegacyProtocols | Unconfiguring IPX crashes the switch |
| CSCsu10229 | Management | The cdpCacheAddress mib not providing GLOBAL_UNICAST Address |
| CSCsw66153 | Management | Native vlan not displayed in show cdp neighbor detail |
| CSCsr50099 | MPLS | show ip explicit-paths command incorrectly displays source route type |
| CSCsv00773 | MPLS | Loose Path Reopt not applied when link costs changed |
| CSCsv41456 | MPLS | Tracebacks seen at IFMGR-3-DUP_IFINDEXifDescr"Virtual-Access2-mpls layer |
| CSCsw35638 | MPLS | FRR Interoperability issue between Juniper PLR and IOS MP |
| CSCsb77148 | Multicast | sh ip mpacket x.x.x.x quality output is wrong after counter wraps around |
| CSCsr82895 | Multicast | watchdog timeout : RP Crash @ igmp_rejoin_groups during RP Switchover |
| CSCsu86494 | Multicast | Assert flag is not cleared after PIM neighbor loss |

| Identifier | Technology | Description |
|---|---|---|
| CSCsu95080 | Multicast | mld_processs block forever in the init_process when parsing config |
| CSCsv29659 | Multicast | RP configured inside the nat not shown on uut outside the nat |
| CSCsx15396 | Multicast | Mcast IIF stays up while physical interface is down |
| CSCsx28948 | Multicast | I/O Memory leak on 7200 |
| CSCsx58861 | Multicast | Crash due to Stack for iGMP process running low |
| CSCsf07760 | PPP | MLP:  Crashes/buffer leaks when large number of sessions come up at once |
| CSCsr81271 | PPP | Invalid VCD error messages upon PVC flap |
| CSCsu70011 | PPP | ipv6 static route pointing to multilink (flexwan) dissapears after sso |
| CSCee63182 | QoS | Router crashes while implementing rate-limit |
| CSCek75808 | QoS | MF: Crash observed at qos_show_policymap_interface_all |
| CSCsl94263 | QoS | Router crash at stile_update_fast_flag due to random-detect dscp-base |
| CSCsm97014 | QoS | Connectivity breaks for QOS + header compression on virtual templates |
| CSCsr05501 | QoS | % NBAR Error: hwidb could not found shows up when reload |
| CSCsv85791 | QoS | Flexwan+/PA-MC-2T3+ introduce 5+ seconds delay on egress |
| CSCed71294 | Routing | Multicast multipath does not work in the vrf context |
| CSCee30355 | Routing | Memory leak at ip_multicast_ctl |
| CSCef65457 | Routing | EIGRP and RIP advertise null0 static routes after they are removed |
| CSCej49366 | Routing | Removing default-metric under EIGRP deletes routes erroneously |
| CSCsb15164 | Routing | Security holes while configuring a standard ACE with host address |
| CSCsd25753 | Routing | BGP Aggregated supernet routes not Advertised properly |
| CSCse68877 | Routing | CEF/BGP table MPLS label mismatch YW3 Non Multi-path |
| CSCsg68717 | Routing | A weird behavior in maxpath configuration in ebgp+ibgp case |
| CSCsh34417 | Routing | BGP Distance not updated following failover to a path with a greater dis |
| CSCsh54161 | Routing | dune, Nov image goes unstable - creates eigrp routing loops |
| CSCsi70484 | Routing | OSPF SPF running constantly if LSID conflicts & prefix filter used. |
| CSCsj13911 | Routing | Cat3750:EIGRP does not receive reply for query between some Vlan |
| CSCsj42399 | Routing | Redistributed static covered by network statement sets metric to 0 |
| CSCsk11930 | Routing | Not able to reconfigure the numbered ip extcommunity-list |
| CSCsk35688 | Routing | Aggregate routes not processed if child routes are deleted pre-maturely |
| CSCsk80250 | Routing | BGP has to handle the return value REXP_DONTKNOW of regexec_hybrid |
| CSCsk87526 | Routing | T/B  ipv6_rib_process_changeQ after shut cmd applied  Int. running RIPng |
| CSCsl32318 | Routing | OSPF: new fix for CSCsk36324 SPF loop |
| CSCsl48075 | Routing | Floating static route behaves incorrectly in 6vPE |
| CSCsl49628 | Routing | VRF is not getting deleted in 'sh vrf' output |
| CSCsl51616 | Routing | v6-vrf-lite config doesn't sync properly with standby |
| CSCsm57494 | Routing | BGP update is not sent after reloading opposite router |
| CSCsm91959 | Routing | Code review: aggregation child routes can miss aggregation logic |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm95129 | Routing | "no ip next-hop-self eigrp" not working when redistribute from BGP |
| CSCsm96901 | Routing | Unable to ping between vrfs through transparent bridge |
| CSCso39597 | Routing | StbyRP crashed @ bgp_vpnv4_bulk_sync_mpls_lbl_binding during bulk sync |
| CSCso51519 | Routing | Paths with same Nexthop selected as multipaths in some sequence |
| CSCso55151 | Routing | ADJ not freeing memory under IPv6 ND stress test |
| CSCso90107 | Routing | SNMP: bgpPeertable and cbgpPeertable shows only results for ipv4 peers |
| CSCsq24935 | Routing | Switch crash due to unsupported bgp/ipv6 command |
| CSCsq43831 | Routing | Stack overflow due to recursion in FIB |
| CSCsq97517 | Routing | C2W2: Mago: CEF on RP is not in sync with SP after reboot. |
| CSCsr01403 | Routing | cefswitching2.1:More time taken(12 mts) to converge after Adjacency flap |
| CSCsr11662 | Routing | EIGRP active routes never go to SIA, queries not sent |
| CSCsr50704 | Routing | dmzlink-bw programs wrong traffic share count in routing table |
| CSCsr51801 | Routing | upon router reload some of the route-maps not permitting the prefixes. |
| CSCsr67361 | Routing | I/O memory leaks when BGP neighbor points to a local address |
| CSCsr86174 | Routing | aggregate-address under address-family does not appear in conf |
| CSCsr90248 | Routing | "aggregate-address advertise-map" not updated dynamically |
| CSCsu06447 | Routing | EIGRP:static route redistribution not working with distribution-list |
| CSCsu11161 | Routing | Neighbor x.x.x.x default-originate issues seen in 12.2 code |
| CSCsu12040 | Routing | PE with CsC configuration sends wrong labels to SPE |
| CSCsu63996 | Routing | OSPF flaps after SSO switchover causes traffic loss after SSO switchover |
| CSCsu76993 | Routing | EIGRP:Routes not tagged with match source redistribution-source |
| CSCsv01474 | Routing | 'ip rip advertise' command lost after interface flap/clear ip route |
| CSCsv05009 | Routing | %OSPF-4-FLOOD_WAR: error during heavy flaps for type-5 and type-7 LSAs |
| CSCsv27607 | Routing | BGP: Outbound route-map updating withdraw only one member |
| CSCsv85052 | Routing | Crash observed when "ispf" is issued in vty with ip routing disabled |
| CSCsv89643 | Routing | OSPF: MAC address of next hop unresolved on ptp eth by adjacency bringup |
| CSCsv97472 | Routing | CSCso62166_dcq_issue_rn_walktree_timed_locking is changed |
| CSCsw24286 | Routing | TE tunnel bandwidth command breaks isis topology |
| CSCsw24826 | Routing | OSPF crash during type-9 maxage |
| CSCsw28893 | Routing | Cost no longer showing with each eigrp route after IOS upgrade |
| CSCsw65441 | Routing | ARP packets drops due to excessive ARP requests sourced from SVI |
| CSCsw65933 | Routing | Prefix not learned from PE to CE |
| CSCsw79397 | Routing | Device crashing at bgp_command_af_specific |
| CSCsx06457 | Routing | BGP may modify routes it does not own |
| CSCsx15841 | Routing | aggregate-address does not NVGEN upon switchover on cat6k |
| CSCsx17446 | Routing | Tunnel route and a non-tunnel (IGP) route with same metric (TE metric) |
| CSCsx51596 | Routing | TCAM ACL entry not correct after removing IP accounting |

| Identifier | Technology | Description |
|---|---|---|
| CSCsx99015 | Routing | crash if OSPF redistributes another OSPF and interface bw changes |
| CSCsy15150 | Routing | 33SXH5: Traceback @ isis_router when default interface configured |
| CSCsy45838 | Routing | show ip ospf border-router crashing router |
| CSCea11368 | Security | CRL fetch using ldap fails if vrf configured in trustpoint |
| CSCeh75136 | Security | TACACS+ rem_addr field empty after first SSH authen attempt fails |
| CSCsc91824 | Security | SSH from router disconnects vty session if there is no matching cipher |
| CSCsv20285 | Security | Whitney:Authentication to the CA server failed using ION. |
| CSCsx15430 | Security | Verbose name lookup calls in IP context causes PKI to block due to pager |
| CSCsx17447 | Security | IOS not including HOST header in HTTP CRL request |
| CSCsy16177 | Security | scp:copy to router over sshv2 fails with  invalid checksum error |
| CSCsy22311 | Security | SCP b/w IOS routers fails while the client is receiving file from server |
| CSCsc67488 | WAN | ARP Req from Frame Relay causes %IP-4-ZERO_ADDR: Zero MAC address Error |
| CSCso62193 | WAN | Standby resets due to parser return error  "no frame-relay vc-bundle" |

## Caveats Resolved in Release 12.2(33)SXH4

### Resolved Infrastructure Caveats

- CSCse85652—Resolved in 12.2(33)SXH4

  **Symptom:** The Cisco IOS HTTP server and the Cisco IOS HTTPS server provide web server functionality to be used by other Cisco IOS features that require it to function. For example, embedded device managers available for some Cisco IOS devices need the Cisco IOS HTTP server or the Cisco IOS HTTPS server to be enabled as a prerequisite.

  One of the functionalities provided by the Cisco IOS HTTP server and the Cisco  IOS HTTPS server is the WEB_EXEC module, which is the HTTP-based IOS EXEC Server. The WEB_EXEC module allows for both “show” and “configure” commands to be executed on the device through requests sent over the HTTP protocol.

  Both the Cisco IOS HTTP server and the Cisco IOS HTTPS server use the locally configured enable password (configured by using the **enable password** or **enable secret** commands) as the default authentication mechanism for any request received. Other mechanisms can also be configured to authenticate requests to the HTTP or HTTPS interface. Some of those mechanisms are the local user database, an external RADIUS server or an external TACACS+ server.

  If an enable password is not present in the device configuration, and no other mechanism has been configured to authenticate requests to the HTTP interface, the Cisco IOS HTTP server and the Cisco IOS HTTPS server may execute any command received without requiring authentication. Any commands up to and including commands that require privilege level 15 might then be executed on the device. Privilege level 15 is the highest privilege level on Cisco IOS devices.

  **Conditions:** For a Cisco IOS device to be affected by this issue all of the following conditions must be met:

  - An enable password is not present in the device configuration
  - Either the Cisco IOS HTTP server or the Cisco IOS HTTPS server is enabled

– No other authentication mechanism has been configured for access to the Cisco IOS HTTP server or Cisco IOS HTTPS server. Such mechanisms might include the local user database, RADIUS (Remote Authentication Dial In User Service), or TACACS+ (Terminal Access Controller Access-Control System)

The Cisco IOS HTTP server is enabled by default on some Cisco IOS releases.

**Workaround:** Any of the following workarounds can be implemented:

– Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an enable password

  Customers requiring the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server must configure an authentication mechanism for any requests received. One option is to use the **enable password** or **enable secret** commands to configure an enable password. The enable password is the default authentication mechanism used by both the Cisco IOS HTTP server and the Cisco IOS HTTPS server if no other method has been configured.

  In order to configure an enable password by using the **enable secret** command, add the following line to the device configuration:

  ```
  enable secret mypassword
  ```

  Replace *mypassword* with a strong password of your choosing. For guidance on selecting strong passwords, please refer to your site security policy. The document entitled "Cisco IOS Password Encryption Facts" explains the differences between using the **enable secret** and the **enable password** commands to configure an enable password. This document is available at the following link:
  http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml

– Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an authentication mechanism other than the default

  Configure an authentication mechanism for access to the Cisco IOS HTTP server or the Cisco IOS HTTPS server other than the default. Such authentication mechanism can be the local user database, an external RADIUS server, an external TACACS+ server or a previously defined AAA (Authentication, Authorization and Accounting) method. As the procedure to enable an authentication mechanism for the Cisco IOS HTTP server and the Cisco IOS HTTPS server varies across Cisco IOS releases and considering other additional factors, no example will be provided. Customers looking for information about how to configure an authentication mechanism for the Cisco IOS HTTP server and for the Cisco IOS HTTPS server are encouraged to read the document entitled "AAA Control of the IOS HTTP Server", which is available at the following link:
  http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml

– Disabling the Cisco IOS HTTP Server and/or the Cisco IOS HTTPS server functionality

  Customers who do not require the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server can disable it by adding the following commands to the device configuration:

  ```
  no ip http server no ip http secure-server
  ```

The second command might return an error message if the Cisco IOS version installed and running on the device does not support the HTTPS server feature. This error message is harmless and can safely be ignored.

Please be aware that disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server may impact other features that rely on it. As an example, disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server will disable access to any embedded device manager installed on the device.

**Further Problem Description:** In addition to the explicit workarounds detailed above it is highly recommended that customers limit access to Cisco IOS HTTP server and the Cisco IOS HTTPS server to only trusted management hosts. Information on how to restrict access to the Cisco IOS HTTP server and the Cisco IOS HTTPS server based on IP addresses is available at the following link:
http://www.cisco.com/en/US/docs/ios-xml/ios/https/configuration/12-4/nm-http-web.html#GUID-BB57C0D5-71DB-47C5-9C11-8146773D1127

Customers are also advised to review the "Management Plane" section of the document entitled "Cisco Guide to Harden Cisco IOS Devices" for additional recommendations to secure management connections to Cisco IOS devices. This document is available at the following link:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

#### Other Resolved Caveats in Release 12.2(33)SXH4

| Identifier | Technology | Description |
|---|---|---|
| CSCef97900 | AAA | AAAA-3-DROPACCTLOWMEM warning message somewhat misleading |
| CSCin45879 | AAA | Router reloaded with radius reorder & dead server & server-private |
| CSCsl29214 | AAA | AAA server change leads to bus error crash after "show run" is issued |
| CSCsl47365 | AAA | TACACS+ authorization should ignore unknown attribute |
| CSCsu21040 | AAA | Enable authentication prompts for username/password instead of just pass |
| CSCsu42152 | AAA | authorization fails if fallback method is "if-authenticated" |
| CSCek37984 | Cisco IOS | Inconsistent BERT behaviour observed on TE1 SPA |
| CSCek40773 | Cisco IOS | CE-CE connectivity broken on MPLS VPN with GRE tunnel in VPN core |
| CSCek71010 | Cisco IOS | TB seen at bgp_oer_notify_pep bgp_oer_remove_path bgp_bestpath_old |
| CSCse12518 | Cisco IOS | MET optimized update can cause blackholing and duplicates |
| CSCsh57238 | Cisco IOS | SXF6:sh int cmd on 6148 cards display zero o/p drops even with qos drops |
| CSCsj04201 | Cisco IOS | %MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC: RP failed allocating IPC buffer |
| CSCsj06641 | Cisco IOS | LI: Traceback found in creating entry in cTap2StreamTable |
| CSCsj32493 | Cisco IOS | IPSEC: Incorrect IPSec connection info in InvalidSPI testing |
| CSCsj51113 | Cisco IOS | crash in ether_cfm_tm_send |
| CSCsj90758 | Cisco IOS | UUT with BGP/DMVPN crashes after restarting iprouting.iosproc |
| CSCsk19866 | Cisco IOS | Unable to boot boomerang image on sup720 |
| CSCsk32209 | Cisco IOS | Crash seen on a stand-alone router while generating RSA keys |
| CSCsk34832 | Cisco IOS | Memory leak in HTTP CORE PID 174 |
| CSCsk73838 | Cisco IOS | After fabric tiemout is seen, line card did not recover using earl patch |
| CSCsk78390 | Cisco IOS | Naxos crashes while trying to fpd upgrade granikos |

| Identifier | Technology | Description |
|---|---|---|
| CSCsk89852 | Cisco IOS | VS2: MEC (LACP) members flap when native subinterface is configured |
| CSCsk94870 | Cisco IOS | VS2: TB @ ether_extract_addr |
| CSCsl02190 | Cisco IOS | ICMPv6 to all node multicast address fail . |
| CSCsl18525 | Cisco IOS | Standby-SP doesn't have mfib table |
| CSCsl27957 | Cisco IOS | %EC-SP-5-CANNOT_BUNDLE2 is seen after inserting WS-SVC-FWM-1 |
| CSCsl32940 | Cisco IOS | Router crashes while reloading Naxos |
| CSCsl37513 | Cisco IOS | SYS-2-MOD_TEMPSENSORFAIL:Module w/ X6148A-GE-45AF and CatOS |
| CSCsl39691 | Cisco IOS | Config Sync:Bulk-sync failure due to Servicing Incompatibility after SSO |
| CSCsl71704 | Cisco IOS | VS2:RACL not applied  on MEC after disabling netflow & chng flowmask |
| CSCsm08087 | Cisco IOS | Arp unresolved after sh/nosh of egress int ;route-map applied at ingress |
| CSCsm08971 | Cisco IOS | SEA:Soft reload occurs everytime after issue show cmd's and T/B with mz |
| CSCsm11898 | Cisco IOS | IOS:SLB: Incorrect NAT Translation when Nat client is enabled |
| CSCsm19550 | Cisco IOS | sup720 rx intr should check tx descriptor exhaustion |
| CSCsm22385 | Cisco IOS | V4 VPN traffic stops after toggling agg. label between vpn-cam and tcam |
| CSCsm26063 | Cisco IOS | C2W2:Active RP Crash on sh/no sh of intf with ipv6 address configured |
| CSCsm28287 | Cisco IOS | Active RP crash on shutdown of GRE tunnel followed by switchover |
| CSCsm40606 | Cisco IOS | WS-X6724 SFP get's reboots again and again with TestSynchedFab Failed |
| CSCsm43962 | Cisco IOS | Cat6k  L2TP packet looped through blocked port |
| CSCsm48287 | Cisco IOS | Drop counters for VPLS VC not incrementing |
| CSCsm64424 | Cisco IOS | C2W1: Copy command generates spurious authorization requests |
| CSCsm65386 | Cisco IOS | WS-X6516A-GBIC card resets on SSO. |
| CSCsm66602 | Cisco IOS | SIP 400 loses VPLS VC entry on shutting down the MPLS TE tunnel |
| CSCsm75286 | Cisco IOS | bgp route-map doesn't work correctly when deleted part of sequences |
| CSCsm79344 | Cisco IOS | Bogus "TCAM MASK entry capacity exceeded" message |
| CSCsm82472 | Cisco IOS | DAI: L2-Portchannel formed for member's DAI trust mismatch |
| CSCsm84267 | Cisco IOS | Tracebacks & %CPU_MONITOR-SP-6-NOT_HEARD: messages with NAT. |
| CSCsm85936 | Cisco IOS | UUT cpu at 40% with bi-dir traffic across a single tunnel |
| CSCso00864 | Cisco IOS | Standby sup crashed on configuing local-address command for cry map |
| CSCso05920 | Cisco IOS | cpmCPUMemoryFree incorrect for Posix memory |
| CSCso18683 | Cisco IOS | IP DSCP Re-circulation not working as expected after issu runversion. |
| CSCso27956 | Cisco IOS | TCAM ASSERT FAILURE on LI stress with add/removal of lots of streams |
| CSCso28275 | Cisco IOS | Traffic polarization within a MEC on VSS. |
| CSCso28791 | Cisco IOS | MAC_MOVE-SP-4-NOTIF seen for L2TP packets over dot1q tunnel |
| CSCso29141 | Cisco IOS | DFC installs drop index for MAC-address |
| CSCso29226 | Cisco IOS | IP source guard is not supported on ether channel member |
| CSCso30038 | Cisco IOS | A OIL is not registerd properly in mroute table with static igmp group |
| CSCso32193 | Cisco IOS | IPv6 software switched in Egress replication mode |

| Identifier | Technology | Description |
|---|---|---|
| CSCso35250 | Cisco IOS | unexpected reload while communicating with CNS server |
| CSCso39818 | Cisco IOS | Ingress Marking not working on SIP-600 on linecard reset/ toggle mlsqos |
| CSCso48665 | Cisco IOS | vlan filter can't be removed totally |
| CSCso49344 | Cisco IOS | Egress policing policy not programmed in SIP-600 after system reload. |
| CSCso57020 | Cisco IOS | VSS: After sso, the RBH values on orphan PO flips w/o link/po flapping |
| CSCso57886 | Cisco IOS | unrestricted while loop when looking for EOS flag in the packet |
| CSCso60528 | Cisco IOS | C2W2: FWSM - Standby FWSM PO shows down and links go down eventually |
| CSCso66357 | Cisco IOS | Classification on nbar fails on removing pmap from other pvc on ATM M2P |
| CSCso71955 | Cisco IOS | Alignment errors with netflow on Interface, crash on 7600/6500 |
| CSCso72178 | Cisco IOS | W2:TestCapture,TestTrap & TestIPv6FibShortcut diag failed ondemand&boot |
| CSCso72541 | Cisco IOS | %MFIB_STATS-DFC2-2-MFIB_STATS_LC_FAILED_GET_COUNTERS for Sip 600 |
| CSCso74559 | Cisco IOS | C2W2: Mago IOS "test Crash" create crashinfo file on bootflash only |
| CSCso85133 | Cisco IOS | DOM tranceiver "voltage" values  are always Zero in SUP4 |
| CSCso86544 | Cisco IOS | Afer SSO, new active SP crashes @ pm_vlan_get_portlist |
| CSCso88042 | Cisco IOS | Wism module Allowed-Vlan statements lost on reload |
| CSCso88772 | Cisco IOS | sp-inband tx capture causes primary SUP to hang |
| CSCso93708 | Cisco IOS | IPsec-HA:RFclient timingout on7200 running 12.4(15)Tx, AdvSecurity fse |
| CSCso98143 | Cisco IOS | Router crash at pm_platform_private_alloc_and_reserve_vlan |
| CSCsq04075 | Cisco IOS | C2W2:DHCP Snooping entries not cleared after removing IP Source Guard |
| CSCsq04274 | Cisco IOS | Memory leak observed on l2_vlan_stat_mem_allocate during vlans creation |
| CSCsq14259 | Cisco IOS | TX Flowcontrol goes on when link negotiation is disabled |
| CSCsq15308 | Cisco IOS | timer not stopped properly for eem policy scripts |
| CSCsq21051 | Cisco IOS | W2: Heathland mode change doesn't work after the second SSO switchover |
| CSCsq26223 | Cisco IOS | WS-X6348-RJ-45 Blackholing traffic/reset continously |
| CSCsq36972 | Cisco IOS | Portchannel does not form.  Log messages indicate misconfig. |
| CSCsq37376 | Cisco IOS | Packet Buffer Capture May Crash a 6500 in IOS |
| CSCsq44850 | Cisco IOS | c2w2 : TB seen at %PM-3-INTERNALERROR: Port Manager Internal Software Er |
| CSCsq46590 | Cisco IOS | Packet loss during SSO failover on ECMP supervisor uplinks |
| CSCsq51231 | Cisco IOS | ALIGN-3-SPURIOUS: Spurious memory access made @ idbman_get_port_swidb |
| CSCsq51249 | Cisco IOS | Monitor session removal may affect traffic through WS-X6148A-RJ-45 |
| CSCsq51378 | Cisco IOS | ATM PA Interface shows up/up after force redundancy, no cables connected |
| CSCsq53085 | Cisco IOS | VS: 15 seconds down time upon module reset |
| CSCsq56747 | Cisco IOS | Active SP CPU 100% after SSO switchover with 080527 ION image |
| CSCsq59297 | Cisco IOS | port-channel IDB gets mixed up |
| CSCsq61089 | Cisco IOS | VS2: physical OIR of 6708 causes 16 seconds interruption |
| CSCsq63727 | Cisco IOS | WS-X6748-GE-TX - input and output errors seen during auto negotiation |
| CSCsq67001 | Cisco IOS | Standy switch reloaded by auto qos on MEC standby member port |

| Identifier | Technology | Description |
|---|---|---|
| CSCsq73317 | Cisco IOS | MAB authorization failed with port-security |
| CSCsq77043 | Cisco IOS | EEM long hostname prevents tcl cli_open from functioning |
| CSCsq77381 | Cisco IOS | W2: Diag - TestL3Capture2 failed after LV-SSO |
| CSCsq78513 | Cisco IOS | VSS: Etherchannel counters incorrect |
| CSCsq78956 | Cisco IOS | strcpy of binary can cause mem corruption |
| CSCsq79253 | Cisco IOS | Pinnacle interrupts not re-enabled after memory inconsistency detected |
| CSCsq80270 | Cisco IOS | Cat 6k crashes randomly after IPSec SPA module is inserted. |
| CSCsq80891 | Cisco IOS | VSS switches reload at the same time after VSL link failure |
| CSCsq81116 | Cisco IOS | c2w2:Device crash @ oer_cc_free_message while unconfiguring |
| CSCsq81235 | Cisco IOS | Cannot configure a vrf again when deleted using 'no ip vrf' command |
| CSCsq82663 | Cisco IOS | SLB router CPU usage is high with GE interface |
| CSCsq82991 | Cisco IOS | IPSG Pacl entry appears after the ISSU RV or SSO |
| CSCsq83219 | Cisco IOS | Standby SP crashed at sp_reset_slcp after "redundancy reload peer" |
| CSCsq83789 | Cisco IOS | LTL for unknow unicast is wrongly programmed for some L3 interfaces |
| CSCsq84116 | Cisco IOS | Cisco 7604 with OC3, Flexwan crashes into ROMMON |
| CSCsq85139 | Cisco IOS | VS2: Can not establish session to standby NAM |
| CSCsq85850 | Cisco IOS | Opnext GLC-LH-SM :remote port stays up when local RX cable is removed |
| CSCsq89415 | Cisco IOS | "no bert" indicates "abort request" instead of "stopped" |
| CSCsq91258 | Cisco IOS | L2 entry purged from hardware when in use by L3 shortcut |
| CSCsq94136 | Cisco IOS | Burst of traffic cause anti-replay check to fail |
| CSCsq94366 | Cisco IOS | Mem leak in rrp_update_peer_info_on_rp |
| CSCsq97640 | Cisco IOS | Resetting Standby Sup4 multiple times causes lincecard switchbus timeout |
| CSCsq98887 | Cisco IOS | Packet drop on applying and removing ACL on tunnel interface with pim |
| CSCsr02723 | Cisco IOS | MDEBUG:Spurious memory access detected at env_sensor_get_update |
| CSCsr02816 | Cisco IOS | ISSU tracebacks seen on SP during runversion at MsgReceive.S:14 |
| CSCsr06914 | Cisco IOS | fm_slb_inbad_send():Invalid Flowmask errors upgrading to 12.2(33)SXH2a |
| CSCsr07565 | Cisco IOS | TCAM didn't reprogram after removing dynamic ACE |
| CSCsr08985 | Cisco IOS | CMM ports going to shutdown state on reload in Whitney 1 |
| CSCsr09554 | Cisco IOS | Move SIBYTE SB_RMON_OVRFL messages under debug |
| CSCsr13633 | Cisco IOS | %PM-3-INTERNALERROR: Port Manager Internal Software E |
| CSCsr18656 | Cisco IOS | BPDU bit is over written when 2nd PCL lookup is enabled. |
| CSCsr18924 | Cisco IOS | kernel idle hook thread in IOS-Base taking 50% CPU |
| CSCsr20679 | Cisco IOS | VSL PO as SPAN source and Orphan PO as SPAN destination not allowed |
| CSCsr26663 | Cisco IOS | C2W2: GLBP 800 peers with default timers flap after SSO |
| CSCsr37131 | Cisco IOS | buginf calls in l2trace when 'debug l2trace' is disabled |
| CSCsr45495 | Cisco IOS | PBR with deny statements : TCAM running out of masks |
| CSCsr45851 | Cisco IOS | ifOperStatus for Control Plane Interface is always down |

| Identifier | Technology | Description |
|---|---|---|
| CSCsr48938 | Cisco IOS | UNBL:bootldr image can't boot on SupW |
| CSCsr49669 | Cisco IOS | Match protcol arp doesnt work in whitney1 earlier it was working for Roc |
| CSCsr51799 | Cisco IOS | pa-mc-8t1 interface down after stopping BERT prematurely |
| CSCsr55523 | Cisco IOS | WCCP service group ID is zero in ACL TCAM Adjacency |
| CSCsr58773 | Cisco IOS | VS2: After SSO, VSL member stuck in "w" state, and MEC errors |
| CSCsr63831 | Cisco IOS | show platform hardware capacity fabric - incorrect % and time-SXH3 |
| CSCsr66588 | Cisco IOS | Netflow SLB aging parameter values are not synced to SP after reload |
| CSCsr72427 | Cisco IOS | WS-X6148-45AF/WS-F6K-FE48-AF %ILPOWER-5-ILPOWER_MISCONFIG after reload |
| CSCsr75094 | Cisco IOS | MDEBUG: Spurious Memory Access on SSO |
| CSCsr78910 | Cisco IOS | time not updated in 'System returned to ROM by reload' in show version |
| CSCsr81962 | Cisco IOS | C2W1: Monitor session servicemodule causes internal loop on SUP720-10GE |
| CSCsr82501 | Cisco IOS | Change global function to static breaks install patch feature in SXH |
| CSCsr93467 | Cisco IOS | c2w2:Traceback seen while doing "switch accept mode virtual " |
| CSCsr96283 | Cisco IOS | High CPU due to add/del SPAN configs |
| CSCsr99933 | Cisco IOS | FWLB: High purge rate causes CPU to increase by 15% |
| CSCsu03297 | Cisco IOS | RE: Fabric force bus-mode does not work anymore |
| CSCsu03772 | Cisco IOS | Dot1q native vlan tagging is not working with "switchpot nonegotiate" |
| CSCsu05800 | Cisco IOS | C2W2: need to extend the wait time for bus sync after sso |
| CSCsu22349 | Cisco IOS | Removing ACL or service policy from vrf interface drops traffic |
| CSCsu24825 | Cisco IOS | SUP32 unstable to communicate with all neighbors after reload |
| CSCsu29117 | Cisco IOS | PE send traffic back to EoMPLS tunnel after lsp path changed |
| CSCsu31651 | Cisco IOS | VSS: Traffic dropped on non-bundled port if RBH=0 |
| CSCsu33221 | Cisco IOS | "Flood in diag inband driver" messages followed by silent reload. |
| CSCsu37481 | Cisco IOS | Netflow Incorrect Octet value with packet-based sampling |
| CSCsu44534 | Cisco IOS | Sup NSF/SSO causes 4 sec traffic loss over EC with uplink ports. |
| CSCsu45210 | Cisco IOS | Upgrade 12.2SXF-> 12.2SXH with Port-Security causes standby boot loop |
| CSCsu46124 | Cisco IOS | SVI ifInMulticastPkts ifOutMulticastPkts are always zero |
| CSCsu48150 | Cisco IOS | Enhancement to Me_Kr register dumps from CSCsg21809 |
| CSCsu49002 | Cisco IOS | ciscoIpMRouteBps sometimes indicates wrongful value |
| CSCsu55635 | Cisco IOS | Load values of PO members with Fixed algo get 0 during bootup on Standby |
| CSCsu57958 | Cisco IOS | DHCP-Snooping not intercepting DHCP messages from the Server |
| CSCsu59556 | Cisco IOS | Traceback seen @ fibidb_init |
| CSCsu63335 | Cisco IOS | "Failed to find process pid" error message on 12.2(33)SXH3 |
| CSCsu64581 | Cisco IOS | Last port of T3/E3 SPA connected back to back does not ping |
| CSCsu68698 | Cisco IOS | No syslogs and stack on console when SP crashes due RP  boot timeout |
| CSCsu69177 | Cisco IOS | C2W2: Traffic drop after SSO on SUP4 P router w/ IP and MPLS traffic |
| CSCsu72496 | Cisco IOS | %PM-3-INTERNALERROR: Port Manager Internal Software Error |

| Identifier | Technology | Description |
|---|---|---|
| CSCsu72884 | Cisco IOS | Modifying match criteria frm v6 to v4 doesnt change tcam label state |
| CSCsu73128 | Cisco IOS | C2W2-ION-080922: Crash on Plain IPSec tunnel setup |
| CSCsu76070 | Cisco IOS | duplicate packets when lawful intercept is enabled |
| CSCsu81785 | Cisco IOS | 6500 can no longer receive the ACL as filter ID from |
| CSCsu82768 | Cisco IOS | Crash at pclc_g2_fw_offline_notification after SSO |
| CSCsu91714 | Cisco IOS | IGMP-JOIN is lost from SUP to MSFC |
| CSCsu94880 | Cisco IOS | Bus error crash at fm_format_inband_adj_data |
| CSCsu95605 | Cisco IOS | Route-map with "match route-type local" not functioning properly |
| CSCsv30359 | Cisco IOS | HSRP: CPU hog when no failover bound to crypto |
| CSCsv34415 | Cisco IOS | Diag failure on power-cycle puts VSS switches in rommon |
| CSCsv43802 | Cisco IOS | High CPU utilization triggers crash in diags. |
| CSCsq31981 | Content | WCCP: redirection does not work with CEF and ip accounting |
| CSCsh45091 | Infrastructure | Port fix for CSCed94684 for ws-c3750-24p |
| CSCsh63508 | Infrastructure | disk0:/sys/cpmbit/base is busy, try again later msg on stby SP on SSO. |
| CSCsi88974 | Infrastructure | LI: Malloc failure on setting MD src interface as Loopback interface |
| CSCsj06593 | Infrastructure | CPU hog msgs for  RFSS worker process and Async write process |
| CSCsj52992 | Infrastructure | CPU hogs when configuring snmp-server host |
| CSCsj54606 | Infrastructure | end of summer-time  can be set earliar than start of summer time |
| CSCsk91176 | Infrastructure | PXF crash causes IPC timeout to all linecards in the chassis |
| CSCsm01126 | Infrastructure | PRE-B crashes while in progress to standby cold-config |
| CSCsm14366 | Infrastructure | Empty crash file generated on wan module crash at boot-up |
| CSCsm32392 | Infrastructure | memory corruption  crash at nv_ifs_open and nv_ifs_close |
| CSCsm47417 | Infrastructure | W2:seting ceExtSysBootImageList cause "wr mem" not working correctly |
| CSCsm78184 | Infrastructure | Switchover failed with %C10KISSU-3-GET_MSG_MTU messages |
| CSCso21611 | Infrastructure | Crash at internal idb counter increment function |
| CSCsq03621 | Infrastructure | Timestamps in "show rmon events" wrap at 2^32-1 milliseconds (7+ weeks) |
| CSCsq16325 | Infrastructure | Incomplete serial interface command creates interface |
| CSCsq34676 | Infrastructure | Modular IOS: show process cpu sorted triggers unexpected reload |
| CSCsq35093 | Infrastructure | XDR-6-XDRIPCNOTIFY: Message not sent to slot 1/0 (1) because of IPC |
| CSCsq60922 | Infrastructure | Modular IOS:Router crashed with SNMP copy and with format in console |
| CSCsr50834 | Infrastructure | CPU HOG after changing logging buffered up to 50MB |
| CSCsr60789 | Infrastructure | W1.3: VSL crash after preemptive switchover in ifs_open_file_decrement |
| CSCsr64361 | Infrastructure | Standby continously resetting due to SNMP RF client notification timeout |
| CSCsu37266 | Infrastructure | Modular IOS: tcp.proc terminated due to signal SIGSEGV |
| CSCsi66366 | IPServices | All transport protocols are displayed in running config for VTY |
| CSCsj83854 | IPServices | Incorrect static nat entries programmed in nat table |
| CSCsm35794 | IPServices | Ignoring Coup after changing HSRP active router's priority |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm79082 | IPServices | RP crash at dispatch_thread_pool when restarting tcp.proc |
| CSCsq60504 | IPServices | Modular IOS Sup720: crashed with tcp timeout logs |
| CSCsq90529 | IPServices | Issue with active ftp on the SXH1 |
| CSCsq97870 | IPServices | Router crash with 'show standby' if group deleted from 2nd terminal |
| CSCsr08771 | IPServices | Crash seen @ dhcpd_pool_nvgen and dhcpd_copy_bootfile |
| CSCsr55990 | IPServices | HSRP mac dynamic on routed pseudowire after reload on active router |
| CSCsu21716 | IPServices | No unsolicited igmp report sent for mroute-proxy |
| CSCsg87930 | LAN | i82543 driver should not increase input queue drop counter |
| CSCsr76818 | LAN | input queue wedge on SP due to VTP packets |
| CSCsh33167 | LegacyProtocols | Dlsw transparent cache holds MAC address for disconnected circuit |
| CSCsq79032 | Management | Excessive remote registry invocation on 'waiting_on_switchover' registry |
| CSCsq84595 | Management | high # of remote reg. invocation (35 rpc/sec) 'get_unidirectional_mode' |
| CSCsr93672 | Management | Native vlan is not getting displayed in "show cdp neighbors" output |
| CSCuk57502 | Management | CDP does not report IPv6 addresses for Modular IOS. |
| CSCsm70668 | MPLS | OIR over E3:POS impacting complete Traffic with biscuit tunnel |
| CSCso21506 | MPLS | Import Map under vrf blocks bgp aggregate prefix |
| CSCsq46044 | MPLS | Error MFI_LABEL_BROKER-3-DELETE_MOI_FAIL and LSD_CLIENT-3-PCHUNK2 |
| CSCsq78822 | MPLS | Cannot clear specific LDP neighbor, when router-id not in bound address |
| CSCsq91960 | MPLS | failed to delete vrf when it is 32 characters long |
| CSCsq93004 | MPLS | Possible memory corruption with TE auto-tunnel primary and subinterface |
| CSCsr40433 | MPLS | mpls te - explicit path with loose nhops - re-optimization failure |
| CSCsu62667 | MPLS | LSP ID change after SSO due to failure in signalling recovered LSP |
| CSCsm77608 | Multicast | IP Multicast packets are Process switched. |
| CSCsr09312 | Multicast | crash when doing mrm stop |
| CSCsr36971 | Multicast | Memory Leak @ PIM process |
| CSCsr49316 | Multicast | Crash ipv6_static_route_find after configured & executed show ipv6 rpf x |
| CSCsu02051 | Multicast | S,G expiry timer change is not allowed in Whitney1 |
| CSCsu71983 | Multicast | Memory Leak @ PIM process |
| CSCsq37078 | PPP | Input errors incrementing on Multilink 5 in admin down state |
| CSCsg18894 | QoS | Queue-limit command should be allowed in conjunction with priority |
| CSCsl62963 | QoS | Router Crashes, Reconfigure a Policy -af_police_remove_coloraware |
| CSCsm00570 | QoS | cwpa2 crashes at hqf_cwpa_pak_enqueue_local |
| CSCsm28515 | QoS | Marking not happening on FlexWAN interface with SXH  after oir/reload |
| CSCsu03813 | QoS | Upgrading from rockies to w2 deletes the police action from pmap |
| CSCsg90755 | Routing | Standby keeps reloading due to PRC mismatch in IPv4 MDT AF config sync |
| CSCsi68795 | Routing | PE wrongly assigns local label to a vpnv4 confederation prefix |
| CSCsj39016 | Routing | warn_assert failed: ../fib/fib_table.c:2947 tal_tree_get_item_count_nonf |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj78403 | Routing | clear ip bgp  causes crash to RR client with conditional route injection |
| CSCsk86150 | Routing | w/ BGP auto-summary enabled, networks are lost from BGP after EIGRP flap |
| CSCsk86476 | Routing | OSPF fails in MTU-mismatch setup when mtu-ignore is configured |
| CSCsm26130 | Routing | BGP with auto-summary not injecting locally orig. route into BGP table |
| CSCsm30569 | Routing | CEF path fragmentation broken for static IPSec VTI |
| CSCsm50741 | Routing | Removal of DCbitless LSA causes problems |
| CSCsm72604 | Routing | OSPF remaining summary route when dual OSPF process redistributing |
| CSCso08786 | Routing | Standby reloads due to config sync failure on inherit peer-policy cmd. |
| CSCso54167 | Routing | BGP peer stuck with table version 0 |
| CSCso80951 | Routing | BGP peers with same policy fall into different update-group with SOO |
| CSCso93535 | Routing | Upon removing a VRF, BGP route timers in other VRF's get reset |
| CSCsq05602 | Routing | TE tunnels are down but still show in the forwarding table |
| CSCsq13938 | Routing | reload on 'show ip bgp vpnv4' when import src delinked by BGP deconfig |
| CSCsq36206 | Routing | MDT tunnels not getting created on 7206 Device |
| CSCsq38431 | Routing | OSPF "summary address" is executed, even if subnet is becoming small |
| CSCsq49201 | Routing | Password in BGP peer-session template not inherited |
| CSCsr67562 | Routing | Support for running ispf with nodes having overload bit configured |
| CSCsr83639 | Routing | Bus error crash when removing BGP configuration |
| CSCsr96042 | Routing | ASR: IOSD crashes at bgp_vpn_import_walker while unconfiguring vrf |
| CSCsu03167 | Routing | SXF15: IPv4/v6 BGP routes not cleared when source routes is gone |
| CSCsu24087 | Routing | Cisco7609 crashes after "clear ip bgp neighbor x.x.x.x soft in" |
| CSCsu36709 | Routing | Unable to boot IOS image on PE (vrf-enabled) router - software fault |
| CSCsu40881 | Routing | Secondary EIGRP address on VRF not added/deleted properly to EIGRP topo |
| CSCeg49153 | Security | PKI: crl checking takes too long to timeout if the server is down |
| CSCsd81870 | Security | Teraterm + TTSSH2 does not work in SSH Ver.2 |
| CSCsf17406 | Security | Large CRLs can cause memory leaks |
| CSCsg48392 | Security | Resuming SSH Session Fails After Disconnecting Another One (Not Console) |
| CSCso48959 | Security | user not reported by "login on-success log" feature for SSH logins |
| CSCsq58748 | Security | IPSEC: IKMP process can get blocked by some PKI  OCSP requests |
| CSCsq60016 | Security | Router crashes when entering a long RSA key string |
| CSCsr85093 | Security | SXF15: SSH session fails withRSA signature verification failed after SSO |
| CSCsr86489 | Security | C6k: SCP file copy causes RP crash during authorization of user |
| CSCsg32308 | WAN | copy/paste of ntp-authentication-key statement is not possible |
| CSCsq18856 | WAN | FR SVCs cannot be setup |
| CSCsq47900 | WAN | OIR operation on POS interfaces with APS result in ALIGN error |

## Caveats Resolved in Release 12.2(33)SXH3a

### Resolved Infrastructure Caveats

- CSCse85652—Resolved in 12.2(33)SXH3a

  **Symptom:** The Cisco IOS HTTP server and the Cisco IOS HTTPS server provide web server functionality to be used by other Cisco IOS features that require it to function. For example, embedded device managers available for some Cisco IOS devices need the Cisco IOS HTTP server or the Cisco IOS HTTPS server to be enabled as a prerequisite.

  One of the functionalities provided by the Cisco IOS HTTP server and the Cisco IOS HTTPS server is the WEB_EXEC module, which is the HTTP-based IOS EXEC Server. The WEB_EXEC module allows for both "show" and "configure" commands to be executed on the device through requests sent over the HTTP protocol.

  Both the Cisco IOS HTTP server and the Cisco IOS HTTPS server use the locally configured enable password (configured by using the **enable password** or **enable secret** commands) as the default authentication mechanism for any request received. Other mechanisms can also be configured to authenticate requests to the HTTP or HTTPS interface. Some of those mechanisms are the local user database, an external RADIUS server or an external TACACS+ server.

  If an enable password is not present in the device configuration, and no other mechanism has been configured to authenticate requests to the HTTP interface, the Cisco IOS HTTP server and the Cisco IOS HTTPS server may execute any command received without requiring authentication. Any commands up to and including commands that require privilege level 15 might then be executed on the device. Privilege level 15 is the highest privilege level on Cisco IOS devices.

  **Conditions:** For a Cisco IOS device to be affected by this issue all of the following conditions must be met:

  – An enable password is not present in the device configuration

  – Either the Cisco IOS HTTP server or the Cisco IOS HTTPS server is enabled

  – No other authentication mechanism has been configured for access to the Cisco IOS HTTP server or Cisco IOS HTTPS server. Such mechanisms might include the local user database, RADIUS (Remote Authentication Dial In User Service), or TACACS+ (Terminal Access Controller Access-Control System)

  The Cisco IOS HTTP server is enabled by default on some Cisco IOS releases.

  **Workaround:** Any of the following workarounds can be implemented:

  – Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an enable password

    Customers requiring the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server must configure an authentication mechanism for any requests received. One option is to use the **enable password** or **enable secret** commands to configure an enable password. The enable password is the default authentication mechanism used by both the Cisco IOS HTTP server and the Cisco IOS HTTPS server if no other method has been configured.

    In order to configure an enable password by using the **enable secret** command, add the following line to the device configuration:

    ```
    enable secret mypassword
    ```

    Replace *mypassword* with a strong password of your choosing. For guidance on selecting strong passwords, please refer to your site security policy. The document entitled "Cisco IOS Password Encryption Facts" explains the differences between using the **enable secret** and the **enable**

**password** commands to configure an enable password. This document is available at the following link:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml

- Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an authentication mechanism other than the default

  Configure an authentication mechanism for access to the Cisco IOS HTTP server or the Cisco IOS HTTPS server other than the default. Such authentication mechanism can be the local user database, an external RADIUS server, an external TACACS+ server or a previously defined AAA (Authentication, Authorization and Accounting) method. As the procedure to enable an authentication mechanism for the Cisco IOS HTTP server and the Cisco IOS HTTPS server varies across Cisco IOS releases and considering other additional factors, no example will be provided. Customers looking for information about how to configure an authentication mechanism for the Cisco IOS HTTP server and for the Cisco IOS HTTPS server are encouraged to read the document entitled "AAA Control of the IOS HTTP Server", which is available at the following link:
  http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml

- Disabling the Cisco IOS HTTP Server and/or the Cisco IOS HTTPS server functionality

  Customers who do not require the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server can disable it by adding the following commands to the device configuration:

  ```
  no ip http server no ip http secure-server
  ```

  The second command might return an error message if the Cisco IOS version installed and running on the device does not support the HTTPS server feature. This error message is harmless and can safely be ignored.

  Please be aware that disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server may impact other features that rely on it. As an example, disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server will disable access to any embedded device manager installed on the device.

**Further Problem Description:** In addition to the explicit workarounds detailed above it is highly recommended that customers limit access to Cisco IOS HTTP server and the Cisco IOS HTTPS server to only trusted management hosts. Information on how to restrict access to the Cisco IOS HTTP server and the Cisco IOS HTTPS server based on IP addresses is available at the following link:

http://www.cisco.com/en/US/docs/ios-xml/ios/https/configuration/12-4/nm-http-web.html#GUID-BB57C0D5-71DB-47C5-9C11-8146773D1127

Customers are also advised to review the "Management Plane" section of the document entitled "Cisco Guide to Harden Cisco IOS Devices" for additional recommendations to secure management connections to Cisco IOS devices. This document is available at the following link:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

#### Other Resolved Caveats in Release 12.2(33)SXH3a

| Identifier | Technology | Description |
|---|---|---|
| CSCsu03167 | Routing | SXF15: IPv4/v6 BGP routes not cleared when source routes is gone |

## Caveats Resolved in Release 12.2(33)SXH3

### Resolved IPServices Caveats

- CSCek52673—Resolved in 12.2(33)SXH3

  A router that has DHCP server enabled could reload after receiving a malformed UDP packet.

  **Workaround:** None

### Resolved Security Caveats

- CSCsi17158—Resolved in 12.2(33)SXH3

  **Symptoms:** Devices running Cisco IOS may reload with the error message "System returned to ROM by abort at PC 0x0" when processing SSHv2 sessions. A switch crashes. We have a script running that will continuously ssh-v2 into the 3560 then close the session normally. If the vty line that is being used by SSHv2 sessions to the device is cleared while the SSH session is being processed, the next time an ssh into the device is done, the device will crash.

  **Conditions:** This problem is platform independent, but it has been seen on Cisco Catalyst 3560, Cisco Catalyst 3750 and Cisco Catalyst 4948 series switches. The issue is specific to SSH version 2, and its seen only when the box is under brute force attack. This crash is not seen under normal conditions.

  **Workaround:** There are mitigations to this vulnerability: For Cisco IOS, the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

  Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with 'ssh' removed from the list of permitted transports on VTY lines while in configuration mode. For example: **line vty 0 4 transport input telnet end**

  If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely using Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html

  More information on configuring ACLs can be found on the Cisco public website: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

### Resolved Unknown Caveats

- CSCsk93241—Resolved in 12.2(33)SXH3

  Cisco IOS Software Multi Protocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi

### Other Resolved Caveats in Release 12.2(33)SXH3

| Identifier | Technology | Description |
|---|---|---|
| CSCdu79630 | AAA | Username on vty not displayed if accounting is not configured |
| CSCsg18288 | AAA | Enable authentication ignores Tacacs+ configuration in rare situation |
| CSCsl10068 | AAA | AAA api migration in login.c, exec.c . |
| CSCsl45701 | AAA | TACACS+ per VRF authen failing: Address already in use |
| CSCsl57645 | AAA | tacacs-server directed-request fails for enable authentication on 6500 |
| CSCso87641 | AAA | Tacacs unable to connect to server |
| CSCso95426 | AAA | Exposure of Radius-Keys in debugs. |
| CSCsq98160 | AAA | No communication between SW and AAA with IPBase image |
| CSCsr26098 | AAA | SSH/Telnet failed with IPBase image on Sup32 with AAA server |
| CSCei33231 | ATM | ATM PVC bundle protected group test failed with bumping exhausted |
| CSCek74474 | ATM | no/default proto ip inarp cmd ineffective until ATM VC bounced. |
| CSCsh98378 | ATM | Router crashes at atm_create_vp_db |
| CSCsi72854 | ATM | Inconsistent IMA CLI after router reload . |
| CSCsk72676 | ATM | Pvc not coming up after removing vc-class from it |
| CSCin67287 | Cisco IOS | NxDS0 BERT capability on PA-MC-8TE1+ |
| CSCsc24015 | Cisco IOS | Parser loops infinitely for match route-type [ext |
| CSCsc85962 | Cisco IOS | Replaying Main Mode packet causing IKE SA deletion |
| CSCsd69625 | Cisco IOS | EZVPN:IOS C876 Client can't connect to ASA using digi certs and noXauth |
| CSCse31572 | Cisco IOS | Bus error at crypto_ikmp_config_authenticated |
| CSCse53517 | Cisco IOS | WiSM: Tracebacks seen after SSO switchover |
| CSCsg22830 | Cisco IOS | Standby not coming up after sso switchover |
| CSCsg87747 | Cisco IOS | RECV_PVID_ERR message received with bringing up etherchannel trunk |
| CSCsh61002 | Cisco IOS | SPA-5X1GE: GE-port not transmitting after 'shut/no shut' and vica versa |
| CSCsi49150 | Cisco IOS | %PM-SP-4-PORT_BOUNCED: Port Gi9/3 was bounced by Consistency Check IDBS |
| CSCsi63649 | Cisco IOS | %SYS-3-TIMERNEG:Cannot start timer with negative offset,TTY Background |
| CSCsi85453 | Cisco IOS | cfg-sync failed  if switchport config is pasted on active & stby restart |
| CSCsi94738 | Cisco IOS | 8xCHT1/E1 SPA modules not in entAliasMappingIdentifier |
| CSCsj37398 | Cisco IOS | Properly initialize the Tycho register AC_QOS_DEFAULT_EGRESS (0x334) |
| CSCsj43677 | Cisco IOS | Active Sup720 crash when removing Standy supervisor |
| CSCsj49293 | Cisco IOS | POS Interface  Output Rate (200 mbps) > Line rate (155 Mbps) |
| CSCsj78820 | Cisco IOS | MEM leak in Crypto IKMP process(crypto_ikmp_author_get_attributes) |
| CSCsj85897 | Cisco IOS | SPA-TE1-Linkrec's out of sync between SPA and LC |
| CSCsj86153 | Cisco IOS | Modular IOS CPU load oscillates even under constant load |
| CSCsj91738 | Cisco IOS | Non-ip packet with mcast-mac addr cause high CPU with VPN-SPA VRF mode. |
| CSCsj94539 | Cisco IOS | Spurious Alarms in PA-MC-8TE1+ may cause router crash |
| CSCsj98198 | Cisco IOS | When we have only 1 flow in TT, flows are not exported to MC |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj98492 | Cisco IOS | Pak subblock handlers need to be part of packet library |
| CSCsk19817 | Cisco IOS | shut/no shut causes pm failed get pm mp semaphore |
| CSCsk67457 | Cisco IOS | BCP-MLP:Traffic stops flowing making one link shut on multilink |
| CSCsk77462 | Cisco IOS | IETF Class attribute is missing in radius accounting record |
| CSCsk88273 | Cisco IOS | Traceback seen @edisms on clearing counter on Active SP |
| CSCsk93366 | Cisco IOS | lte_rp_get_lte_update_xdr_size/fib_upd_consume_rec_meets_upd_rec crash |
| CSCsl04386 | Cisco IOS | %BIT-STDBY-4-OUTOFRANGE : Traceback on Bootup . |
| CSCsl06059 | Cisco IOS | Router crash at route_map_vrf_af_change_nh |
| CSCsl11335 | Cisco IOS | MVPN-MIB:Entries obtained from "ciscoMvpnBgpMdtUpdateTable" is incorrect |
| CSCsl11868 | Cisco IOS | With IP CEF enabled ACL is not denying packets as intended. . |
| CSCsl17798 | Cisco IOS | Etherchannel state inconsistent between active and standby |
| CSCsl28371 | Cisco IOS | SPA-IPsec-2G VRF: L2 loop and broadcast storm may occur on default vlans |
| CSCsl34481 | Cisco IOS | IPV6-MCAST:router crashes while unconfiguring ipv6 mcast routing |
| CSCsl35325 | Cisco IOS | MRIB client remains after a linecard removal |
| CSCsl39710 | Cisco IOS | cat6000 mac-address-table does not add entries for local fwsm mac . . |
| CSCsl40528 | Cisco IOS | VS2: Port-channel fails to forward unicast packets after switchover . |
| CSCsl53494 | Cisco IOS | C7600-SSC-400: Error message display incorrect product name |
| CSCsl53727 | Cisco IOS | Add UDLD interface counters for debugging purpose |
| CSCsl61164 | Cisco IOS | Router may crash @ipflow_fill_data_in_flowset when changing flow version |
| CSCsl69123 | Cisco IOS | SIP-400:QoS:Police drops MPLSCP, CDPCP negotiation packets - SRA,SRB |
| CSCsl70667 | Cisco IOS | 12.2(33)SRB2: LC crash at fib_fib_feature_space_xdr_decode |
| CSCsl72912 | Cisco IOS | VS2: WS-X6708 DFC crash in local_cb1(Segment violation) |
| CSCsl80682 | Cisco IOS | SPA crashes if crypto acl changed |
| CSCsl89890 | Cisco IOS | VS2: crash in psecure-process_timer |
| CSCsl93559 | Cisco IOS | Unsupported ISL encap CLI option should be disabled on 6716 |
| CSCsl94393 | Cisco IOS | OPNEXT / Sup32 uplink port stays up when far-end port down. |
| CSCsl98238 | Cisco IOS | QoS statistics-export only exports to directly-connected destinations |
| CSCsm04256 | Cisco IOS | CPUHOG and crash after 'show memory detailed all statistics' issued |
| CSCsm24906 | Cisco IOS | IPV6 neighbour discovery not working on SVI intf under VRF |
| CSCsm32363 | Cisco IOS | Netflow SLB sw-installed entries not aging out |
| CSCsm37673 | Cisco IOS | Traffic from SSLM service module not going over multi-module etherchanne |
| CSCsm54873 | Cisco IOS | EEM some time are not triggered properly |
| CSCsm56279 | Cisco IOS | C2W2: Important enhancements to "test swi vir ltl index" CLI |
| CSCsm59039 | Cisco IOS | Message "ME_AR#0 WARNING: Cannot FLUSH Dic#0" seen for WS-X6708A-10 LC |
| CSCsm59384 | Cisco IOS | DPD not deleting IKE SA's |
| CSCsm59926 | Cisco IOS | RP receives 2 copies of each PIM register with MVPN |
| CSCsm59949 | Cisco IOS | vtp3:with 4k vlan HA reload/sso causes the standby to reload continuosly |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm69112 | Cisco IOS | Multicast output drop w/ IGMP snooping @ near line rate 1Gbps |
| CSCsm69827 | Cisco IOS | %SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3 |
| CSCsm70707 | Cisco IOS | WS-X6748-SFP shutdown(Could not set appropriate Switching mode) |
| CSCsm70774 | Cisco IOS | Router crashes at cfg_kron_plcy_sbmd_cmd. |
| CSCsm71537 | Cisco IOS | divide by 0 crash in oer_br_update_iface_counters |
| CSCsm72807 | Cisco IOS | DHCP packets can get corrupted in an SSO environment |
| CSCsm75020 | Cisco IOS | EARL7 Additional ECC Error Handling enhancements |
| CSCsm76111 | Cisco IOS | 10G ports generate CRC errors when using CISCO-FINISAR transceivers |
| CSCsm77171 | Cisco IOS | Router crash when "ip flow" enabled. |
| CSCsm77923 | Cisco IOS | C6k: Invalid vlan iface order in config after new vlan iface addition |
| CSCsm82264 | Cisco IOS | VS2: Entire VSS system goes down after restarting call-home process |
| CSCsm82958 | Cisco IOS | radius sticky entry deleted even if the idle timer is not 0 |
| CSCsm84257 | Cisco IOS | crash in ipflow_periodic context due to watchdog timeout |
| CSCsm86027 | Cisco IOS | B2B failover,ace_tunnel_compare:Invalid address_type, router crashed |
| CSCsm94421 | Cisco IOS | Configuring STP cost in an etherchannel to the defaulthas no effect |
| CSCsm99170 | Cisco IOS | Memory Leak seen in fw_lcp process |
| CSCsm99690 | Cisco IOS | Netflow: Crash with aggregation caches and export to MPLS VPN |
| CSCso00793 | Cisco IOS | ITP-76: Flexwan Memory version "VI4DP647228EBK-MD" causes reload |
| CSCso05127 | Cisco IOS | WS-X6708-10GE crashes following upgrade to 12.2(33)SXH1 and 12.2(33)SXH2 |
| CSCso08224 | Cisco IOS | WS-X6148-45AF port link takes 8 or more seconds to come up |
| CSCso13950 | Cisco IOS | implementation of cmasModuleActionNotif in CSICO-MODULE-AUTO-SHUTDOWN-M |
| CSCso16973 | Cisco IOS | VC in PE2 stays UP even after disabling ip cef globally |
| CSCso17569 | Cisco IOS | VPN-SPA: WAN interface mtu incorrectly programmed on the SPA |
| CSCso19924 | Cisco IOS | VPN SPA Module: Performance degradation on none-fragmented packets |
| CSCso20519 | Cisco IOS | Cheronia: Fix SMB drive strength programming. |
| CSCso20978 | Cisco IOS | EEM cron timer events save internal timer names to the config |
| CSCso22754 | Cisco IOS | MAB/802.1X interop busted |
| CSCso31506 | Cisco IOS | IPv6 AH Extension Headers Punted to Software on PFC-3B & 3C |
| CSCso37640 | Cisco IOS | DHCP snooping ACL's are not getting programmed after switchover. |
| CSCso38151 | Cisco IOS | Error/Traceback after power fail. %SPA-3-SW_ERROR: spa_get_card_info: |
| CSCso39444 | Cisco IOS | The new Active supervisor will crash after SSO @ fib_path_list_lock_memo |
| CSCso39518 | Cisco IOS | fh_policy_dir.proc process crash when activate 0E patch |
| CSCso43539 | Cisco IOS | power converter failure reported before power was on |
| CSCso44072 | Cisco IOS | High CPU due to multicast traffic getting punted to software |
| CSCso46210 | Cisco IOS | VS: NAM on Standby switch not able to configure SPAN session |
| CSCso50175 | Cisco IOS | % ENT_API-4-NOPORT: Traceback seen after switchover |
| CSCso51417 | Cisco IOS | Enabling Gigabit ports on RSP720 cause send/receive of BFD packets fail |

| Identifier | Technology | Description |
|---|---|---|
| CSCso52097 | Cisco IOS | IPV6 :Missing second Netflow shortcut after route change |
| CSCso53741 | Cisco IOS | VPNSPA does not handle duplicate IPSec SA correctly in nested tunnel |
| CSCso54131 | Cisco IOS | After SSO BPDU are being dropped |
| CSCso55072 | Cisco IOS | Crash occurs during execution of TCL code in ESM handler |
| CSCso56644 | Cisco IOS | EEM2.3::%SYS-3-CPUHOG: EEM ED Interface |
| CSCso59288 | Cisco IOS | On enabling oob, aging is changed to 3 times is not shown in cli output |
| CSCso62526 | Cisco IOS | c7600 RSP720: stdby RSP relods upon no flow-sampler interface commad |
| CSCso65821 | Cisco IOS | wrr-queue map configuration propagates to all ports on a 6408 |
| CSCso68840 | Cisco IOS | eou inactivity timer over rides reauth timer from ACS |
| CSCso71355 | Cisco IOS | PVLAN - 6500 - Multicast flood broken from pvlan port to promiscuous |
| CSCso75657 | Cisco IOS | Unable to configure cwan int in SSO - standby doesn't support cmd |
| CSCso82039 | Cisco IOS | C2W2: Active console is getting locked for 2.5 mins during sso. |
| CSCso84567 | Cisco IOS | 6500 with WCCP and CoPP punts non-TCP packets into CoPP policy. |
| CSCso85859 | Cisco IOS | RP crashs when using 'show memory detailed' |
| CSCso87348 | Cisco IOS | Corruption in subflow code |
| CSCso87838 | Cisco IOS | HSRP: with aggressive timers HSRP peer flaps when "wr mem" |
| CSCso89823 | Cisco IOS | Pos interface "rxload" and "input bytes" counters incorrectly increment |
| CSCsq00884 | Cisco IOS | "mls qos trust" cmd lost under port-channel interface when upgrading IOS |
| CSCsq03475 | Cisco IOS | W2: Memory corruption caused by env object after being freed. |
| CSCsq04355 | Cisco IOS | Fix in CSCso81632 is not complete |
| CSCsq04673 | Cisco IOS | SIGSEGV in ios-base and syslog_pubinfo_enqueue |
| CSCsq09228 | Cisco IOS | CHSTM1 SPA: Linkup/down traps not generated and snmp set not working |
| CSCsq19146 | Cisco IOS | FPD creation for new pegasus rx (1.6) FPA image for Sip-1 CR |
| CSCsq20970 | Cisco IOS | ATM option missing, while configuring T1 controller for mode atm |
| CSCsq33790 | Cisco IOS | Switch crashes when authenticating a user with Filter-Id attribute |
| CSCsq34245 | Cisco IOS | IPC Open Port Errors observed with SIP-400 |
| CSCsq39079 | Cisco IOS | SPA-IPSEC-2G Crash under load due to IKE session establishment |
| CSCsq46327 | Cisco IOS | Ca6k SXH : 2 crypto maps in same redundant standby grp: RRI not deleted |
| CSCsq47140 | Cisco IOS | 67xx module may not come online |
| CSCsq47305 | Cisco IOS | High CPU on SP when both VSL PO are source interface |
| CSCsq51286 | Cisco IOS | Memory Leak Occuring in QM Process on RP when a port is shut/no shut |
| CSCsq53822 | Cisco IOS | Monitor session removal may affect traffic through WS-X6148A-RJ-45 |
| CSCsq60553 | Cisco IOS | Create cwslc-rommon3.bin for cwpa2 to accomodate release Rommon (1.8) |
| CSCsq62351 | Cisco IOS | C2W2:SUPW: GOLD EEM cannot crash switch immdediately as recovery action |
| CSCsq63019 | Cisco IOS | Router Crash when "Clear Crypto Sessions" is issued on EzVPN server |
| CSCsq63681 | Cisco IOS | c7600 Router crashing due to freed pointer in cfib invoked by Netflow |
| CSCsq74300 | Cisco IOS | Set interface change for CSCsk63775 needs to be backed out |

| Identifier | Technology | Description |
|---|---|---|
| CSCsq75704 | Cisco IOS | FW2 FE PA Interface stays up/down with no conn and goes up/up after sso |
| CSCsq76749 | Cisco IOS | System Crash when inserting 10G Cards |
| CSCsq77464 | Cisco IOS | mls rate-limit unicast cef receive value re-written upon TCAM exception |
| CSCsq87431 | Cisco IOS | tracebacks seen on issuing sh mls qos ip command |
| CSCsq87833 | Cisco IOS | platform ipv6 acl ahp command rejected during bootup |
| CSCsq90487 | Cisco IOS | ME6524 running modular IOS images require 512 MB DRAM in SP in SXH3 |
| CSCsq94150 | Cisco IOS | VSS system crash on show command during the initial conversion |
| CSCsr12976 | Cisco IOS | High CPU in ION ios-base process |
| CSCsr28305 | Cisco IOS | Packet drops on L2 portchannel on WS-X6708-10G |
| CSCek58956 | Infrastructure | Need process_ok_to_reschedule check in process_may_suspend |
| CSCsa97971 | Infrastructure | IOS SLB TCP probe state toggles |
| CSCsb06920 | Infrastructure | SYS-3-MGDTIMER: Running timer -Process= SAA Event Processor |
| CSCsd37499 | Infrastructure | %IFS-3-FSMAX: Failed to add ?, maximum filesystems 64 msg with Traceback |
| CSCsh96179 | Infrastructure | IPSLA pathEcho probe doesn't complete for all hops |
| CSCsj52693 | Infrastructure | ospf neighbor flap with fast hellos and 16 neighbors |
| CSCsk70446 | Infrastructure | NRT: tracebacks @ data_inconsistency_error - 7200 for HTTP config . |
| CSCsk99687 | Infrastructure | crash seen during ISSU runversion in ipc_open_port |
| CSCsl60092 | Infrastructure | Active SP crashed @ipc_fragment_cleanup with VSL shut/no shut test |
| CSCsm49218 | Infrastructure | Missing traceback for jump to zero exceptions |
| CSCsm77199 | Infrastructure | DATACORRUPTION-1-DATAINCONSISTENCY HTTP_FIND_FLASH_FILE |
| CSCsm89735 | Infrastructure | Router crashes on giving show idb after sessions are down in PPPOE-ipv6 |
| CSCso02960 | Infrastructure | %RTT-4-DuplicateEvent causes trackbacks after upgrading to 12.2(33)SXH |
| CSCec51750 | IPServices | Router reloads do to bus error. and illegal access to low address |
| CSCeh69721 | IPServices | %SCHED-3-CORRUPT:Schedulerevent magic corrupted by TFTP Server |
| CSCsb85982 | IPServices | Router reloads@ add_or_create_more_soc_buckets |
| CSCsi42225 | IPServices | We need improvement for ip igmp limit command |
| CSCsk83505 | IPServices | %L3_MGR-3-REQ_SEND:error packet allocation after Remote HL HW reset |
| CSCsk96976 | IPServices | DHCP Option 66 adds more quotation marks around URL after reload . |
| CSCsl51945 | IPServices | HSRPv6: Config Sync and stanby resets with standby 1 ipv6 <> |
| CSCsm59037 | IPServices | no service dhcp command causes switch to reload |
| CSCsm70580 | IPServices | c2w2:ciscoFtpClientMIB: ftp_fs.proc extra processes can deadlock & crash |
| CSCsm92206 | IPServices | Router crashes when set the range of interfaces to default configs |
| CSCso68344 | IPServices | Switch acting as DHCP server crashes on issuing no service dhcp command. |
| CSCso91230 | IPServices | %LINK-2-INTVULN: errors with MLPPP and HWIC-4ESW |
| CSCsq14698 | IPServices | crash when using nat with multicast traffic |
| CSCsq48201 | IPServices | c7300:Bridge IRB-Router crash and traffic flow issue |
| CSCsq67478 | IPServices | SSH session hangs |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl54243 | LAN | 7600 SIP-400 crash after removing sub-ints; lc_deencap_dot1q_vlan |
| CSCeh97382 | Management | Device reset when polling IKE/IPSEC MIB |
| CSCsk38681 | Management | VS2: remote registry call messages ~ cdp2.iosproc:1 |
| CSCsq79132 | Management | Excessive remote registry invocation on 'proto_on_swidb' registry |
| CSCsj50412 | MPLS | Improper handling of remote binding wrt route info |
| CSCsk42307 | MPLS | MPLS-TE CBTS: Sending out OSPF hellos over master tunnel . |
| CSCso53377 | MPLS | All TE Lsps does not recover after SSO switchover |
| CSCek75931 | Multicast | LNS: %SYS-3-CPUHOG When sessions  have multicast |
| CSCsk26429 | Multicast | Router configured for IGMP Proxy may not send IGMP Join |
| CSCsl10316 | Multicast | ipv6 pim join-prune-interval 10 sets the interval to 20 seconds . |
| CSCsl20158 | Multicast | SNMP:msdpPeer counters should be able to compare with CLI counters. |
| CSCsl92316 | Multicast | LNS: %SYS-3-CPUHOG when clear l2tp tunnel, sessions have multicast |
| CSCsm17426 | Multicast | RP-bit not cleared on s,g; traffic outage for 4 minutes |
| CSCsm44620 | Multicast | Shutdown interface present in PIM interface list |
| CSCsm48322 | Multicast | IPv6 Multicast RP ignores embedded RP register messages |
| CSCsm53766 | Multicast | Reload due to Address Error with multicast configuration |
| CSCsq09962 | Multicast | 7600 : crash at "pim_proxy_empty_rd" |
| CSCsq14151 | Multicast | RPF of (S,G) is set to NULL, When (S, G, R) entry is convered to (S, G) |
| CSCse40966 | PPP | MLP links down after SSO switchover if aaa new-model cfged |
| CSCek63203 | QoS | CEOP:VH:Ctrl+C while display show policy int cause console freeze |
| CSCsm29181 | QoS | Crash when NBAR applied to sub-interface |
| CSCsm49062 | QoS | cwan2: show queueing interface reports double count for wfq drops |
| CSCek36995 | Routing | 0.0.0.0 default route increasing on rip DB with object tracking |
| CSCse65277 | Routing | MU:default isis metric maximum returns parser error |
| CSCsf06946 | Routing | Removing loopback interface causes continuous standby RP reloading |
| CSCsi87894 | Routing | RIP advertise default route after 'no default-information originate' |
| CSCsi98730 | Routing | CEF/BGP table MPLS label mismatch in IOS 12.4(6)T5 |
| CSCsj21785 | Routing | TE tunnel does not reoptimize after mtu change |
| CSCsj56281 | Routing | BGP inherit peer-policy not working after router reload |
| CSCsk37659 | Routing | Vrf route table does not get updated once pppox sessions are up. |
| CSCsl04835 | Routing | BGP conditional route injection not removing routes from iBGP peers |
| CSCsl06336 | Routing | removing 'maximum-paths import 6' causes duplicate paths in VRF table |
| CSCsl20856 | Routing | standby HSRP flaps with ospf mib polling/aggressive timers/nostandby sso |
| CSCsl30331 | Routing | Prefixes permitted despite the deny action on route-map continue |
| CSCsl72774 | Routing | Memory leak in CEF consistency checker |
| CSCsl84712 | Routing | Error- %OSPF-4-FLOOD_WAR: Process 123 re-originates LSA ID 10.55.122.148 |
| CSCsl92283 | Routing | Unable to add into routing table if static route use interface + gateway |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm04442 | Routing | Router crash at rip_find_sum_idb |
| CSCsm39159 | Routing | ARP HA cpu hog on stby while bringing up stby with large arp tables |
| CSCsm43938 | Routing | stby resets when large config/arp table to sync over to it |
| CSCsm45634 | Routing | BGP VPNv4 route is not actived immediately after receving update |
| CSCsm47111 | Routing | FIB: Accessing freed memory while dequeuing |
| CSCsm91801 | Routing | ASBR not updating metric in LSA-5 redistributing from 2-nd OSPF process |
| CSCsm96785 | Routing | "nsf cisco" under router ospf config does not work, but "nsf ietf" works |
| CSCso00383 | Routing | MVPN: New style PE doesn't send  RD Type 2 MDT update |
| CSCso27510 | Routing | Removing SVI with IPv6 address with 'no int vlan' crashes the router |
| CSCso30199 | Routing | ISIS topology broken after a force-switchover when ispf is enabled |
| CSCso62166 | Routing | Crash @ bgp_netlist_validate when ibgp established with metric |
| CSCso63693 | Routing | ISIS: Maximum circuit limit (255) has reached with passive-interface def |
| CSCso64274 | Routing | 0.0.0.0/0 redistributed entry not removed RIP DB after deleting command |
| CSCso73076 | Routing | can not delete ACE enties in ACL |
| CSCso89675 | Routing | Device crash @  ip2access_add_pbacl_item with largre PBACL configuration |
| CSCsq62703 | Routing | Router crashed with TLB (load or instruction fetch) exception |
| CSCsq75944 | Routing | crashes in ipflow_ager, ipflow_sub functions, ipflow_periodic |
| CSCeh48777 | Security | tunnel interface fluctuates between UP/DOWN state during ipsec rekey |
| CSCir01449 | Security | Sync damage of CSCin74155 fix |
| CSCsb58633 | Security | SCP server gives files with invalid checksum on some router platforms |
| CSCsb80803 | Security | SSH Process: SCHED-3-UNEXPECTEDEVENT error message |
| CSCse12154 | Security | Bus error crash after executing secure copy (scp) |
| CSCsk75078 | Security | rcv client_input_channel_req: channel 0: unknown channel |
| CSCsl61311 | Security | New SSH sessions with RSA key sometimes fails after changing  hostname |
| CSCsm57122 | Security | Scp and ssh failing with certain ssh clients |
| CSCsl90285 | WAN | POS-APS: CWPA-3-NODISPATCH messages seen when configuring APS |

## Caveats Resolved in Release 12.2(33)SXH2a

| Identifier | Technology | Description |
|---|---|---|
| CSCsl45701 | AAA | TACACS+ per VRF authen failing: Address already in use |
| CSCso87641 | AAA | Tacacs unable to connect to server |
| CSCsh61002 | Cisco IOS | SPA-5X1GE: GE-port not transmitting after 'shut/no shut' and vica versa |
| CSCsm69827 | Cisco IOS | %SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3 |
| CSCso05127 | Cisco IOS | WS-X6708-10GE crashes following upgrade to 12.2(33)SXH1 and 12.2(33)SXH2 |
| CSCso53516 | Cisco IOS | VSS: Incorrect fpoe programming causing unicast traffic blackhole |

## Caveats Resolved in Release 12.2(33)SXH2

### Resolved Security Caveats

- CSCsj85065—Resolved in 12.2(33)SXH2

  A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Cisco has released free software updates that address this vulnerability. Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl.

### Resolved Unknown Caveats

- CSCsg35077—Resolved in 12.2(33)SXH2

  **Symptoms:** A device that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message.

  **Conditions:** The device must have a valid and complete configuration for IPsec. IPsec VPN features in Cisco IOS software that use IKE include Site-to- Site VPN tunnels, EzVPN (server and remote), DMVPN, IPsec over GRE, and GET VPN.

  **Workaround:** Customers that do not require IPsec functionality on their devices can use the **no crypto isakmp enable** command in global configuration mode to disable the processing of IKE messages and eliminate device exposure.

  If IPsec is configured, this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.

  Further Problem Description: This bug is triggered deep into the IKE negotiation, and an exchange of messages between IKE peers is necessary.

  If IPsec is not configured, it is not possible to reach the point in the IKE negotiation where the bug exists.

### Other Resolved Caveats in Release 12.2(33)SXH2

| Identifier | Technology | Description |
|---|---|---|
| CSCee66606 | AAA | per-group deadtime is nvgend as 60x user input |
| CSCee89849 | AAA | Router  reloaded at vtemplate_build_command_strings |
| CSCsc98046 | AAA | TACACS Accounting isn't sending stop time in the stop packet. |
| CSCsd48175 | AAA | AAA/TACACS not failing over to second server |
| CSCsg14301 | AAA | AAA/TACACS spurious memory accesses in tplus_handle_req_timeout |
| CSCsj88665 | Access | Bus error with PA-MC-2T3+ when deleting channel-group |
| CSCsl41784 | Access | ION: ARP Input memory leak with "mobile ip arp" |
| CSCsd84347 | ATM | PVC stops sending OAM loopback if AIS/RDI  received |
| CSCsj84931 | ATM | CEOP: after OIR with atm local switching and ima, router crashes |

| Identifier | Technology | Description |
|---|---|---|
| CSCeb69473 | Cisco IOS | connect '/terminal-type' command memory corruption |
| CSCeh08262 | Cisco IOS | Show tech SP output should honor redirect applied |
| CSCek53174 | Cisco IOS | dhcp snooping cannot scale beyond 225 bindings |
| CSCek66116 | Cisco IOS | B2B: IKEA trans 0x17; opcode 0x53; param 0x41 msg displayed forever |
| CSCek71816 | Cisco IOS | CE-CE ping fail after restore ASBR-PE vrf |
| CSCek78874 | Cisco IOS | KMI:Out of order deletes cause sync issues |
| CSCsb87956 | Cisco IOS | loop  in the state  IKE_CONFIG_MODE |
| CSCsh17328 | Cisco IOS | WS-SVC-WISM-1-K9 reports 0.0 in entPhysicalVendorType |
| CSCsh84657 | Cisco IOS | STP Loopguard: Ability to disable loopguard for Po270 and higher for FWM |
| CSCsh97395 | Cisco IOS | IDSM: Monitor config was removed after RPR switchover |
| CSCsi52382 | Cisco IOS | radius attribute 5 nas-port not sent in access-request for RA VPN users |
| CSCsi97434 | Cisco IOS | A router may crash when ipsec is established |
| CSCsj48453 | Cisco IOS | AW: CAT6k does not forward multicast traffic to WISM in L3 mode |
| CSCsj68951 | Cisco IOS | Diag Minor Error: TestVslStatus by shut down one side Sup4 uplink |
| CSCsj87584 | Cisco IOS | call-home inventory full needs show ipdrom switch all for VSS |
| CSCsj91961 | Cisco IOS | Ifnums of channels for E3 dont match on active and stdby |
| CSCsk16240 | Cisco IOS | C2W1: active not responding msgs seen om reload with 41patches |
| CSCsk21354 | Cisco IOS | PAT : Missing second Netflow shortcut after route change. |
| CSCsk27081 | Cisco IOS | ifHCInOctets and ifHCOutOctets on GE-WAN interfaces wrap up at 2^32 |
| CSCsk32872 | Cisco IOS | Wrong API usage, can lead to crash . |
| CSCsk33740 | Cisco IOS | replay window size of 1024 causes IPSec Policy Check and Replay Failure |
| CSCsk41134 | Cisco IOS | ISAKMP SA neg not successful for in tunnel mode w/ RSA-SIG |
| CSCsk44233 | Cisco IOS | While raising the interrupt level, bgp_route_map_inform tries to suspend |
| CSCsk58040 | Cisco IOS | WS-X6148A-GE-45AF retains previous modules MACs after OIR |
| CSCsk80552 | Cisco IOS | Shut and no shut of interface causes the delay in forming rp mapping |
| CSCsk82370 | Cisco IOS | RP crash and tracebacks in crypto related process |
| CSCsk83089 | Cisco IOS | Increase maximum aggregate policer > 10Gbps |
| CSCsk84925 | Cisco IOS | ipv4:SSM mroute not created due to ip mr-cache on IIF, traffic hits MSFC |
| CSCsk97144 | Cisco IOS | wait for remote process DiagCard7/-1creation times out with 1018 ION |
| CSCsl06577 | Cisco IOS | Linking bootflash to bootdisk failed after  pcmcia_driver.proc restart |
| CSCsl12827 | Cisco IOS | Handling Transit IpSec in VRF mode |
| CSCsl18765 | Cisco IOS | 6500-7600 : SPAN of EoMPLS port causes packet reflection or loop |
| CSCsl19708 | Cisco IOS | Naxos : Disable Telesto Internal TERMINATION For Reference Clock, PB RAM |
| CSCsl27236 | Cisco IOS | %SYS-3-CPUHOG: Task is running for (126000)msecs, causes RP crash . |
| CSCsl32344 | Cisco IOS | Group of 4 ports on 6708 stops passing traffic |
| CSCsl34515 | Cisco IOS | VS2:after SSO with preemption, port security is broken |
| CSCsl43540 | Cisco IOS | VS2:snmp mac notification for port channel on DFC linecard doesn't work |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl51380 | Cisco IOS | Sup720 and Sup32 TCAM & SSRAM Consistency Checkers refinement |
| CSCsl51395 | Cisco IOS | slot_earl_icc_shim_addr:device crash with hw-module reset |
| CSCsl52092 | Cisco IOS | DHCP db agent considers port-channel interface (poX) as invalid |
| CSCsl53037 | Cisco IOS | Mail action does not separate headers from body |
| CSCsl53845 | Cisco IOS | sup720/SXH: dummy packet send over inband when sw netflow is used |
| CSCsl58673 | Cisco IOS | EEM Prevents VTY telnet to MCP router |
| CSCsl58924 | Cisco IOS | Standby SP crashed due to TestAclDeny failure on bootup/switchover |
| CSCsl59553 | Cisco IOS | SIP-400: bursty traffic causes packet drop even in low rates |
| CSCsl63311 | Cisco IOS | 6500 May Experience High CPU due to NAT traffic |
| CSCsl70016 | Cisco IOS | WS-X6516A-GBIC card in switch 2 goes down frequently in vsl |
| CSCsl70404 | Cisco IOS | Memory leak on SUP - CMFI Process |
| CSCsl71339 | Cisco IOS | Prevent ssa interrupts from corrupting sfp i2c accesses |
| CSCsl72752 | Cisco IOS | VS2: after preempted switchover, interface states are out of sync |
| CSCsl74456 | Cisco IOS | VPN-SPA : TCAM not programmed on POS sub-interface after a reload |
| CSCsl74976 | Cisco IOS | Punted MPLS-tagged traffic causes control plane instabilities |
| CSCsl75136 | Cisco IOS | Cat6k with Sup32 failed to boot up after power cycle. |
| CSCsl75719 | Cisco IOS | sxf13 show int tunnel with blank display |
| CSCsl75836 | Cisco IOS | VS2: MCAST LTL T/B's observed, when removing VLAN / SVI used for mcast |
| CSCsl76647 | Cisco IOS | VPN SPA Cannot clear SA using conn-id with CLI |
| CSCsl79219 | Cisco IOS | mvpn : bidir shadow entries not installed |
| CSCsl83211 | Cisco IOS | Sup32 running ION image fails to bootup after a power-cycle. |
| CSCsl84317 | Cisco IOS | Active crashes on applying acl to EoMPLS subif on SIP-600 |
| CSCsl89069 | Cisco IOS | Zamboni crashed at illegal event/state combinationin CfgMonInd, clear sa |
| CSCsl89176 | Cisco IOS | Cat6k may crash when vlanTrunkPortEntry is polled via snmp |
| CSCsl89425 | Cisco IOS | BFD sessions dont scale |
| CSCsl91085 | Cisco IOS | system/iprouting.iosproc crash after activate 39 dummy/restart patches |
| CSCsl92286 | Cisco IOS | 60 second multicast traffic loss as VSS standby chassis initializes |
| CSCsl94301 | Cisco IOS | VS2: Mac learning in linecard gets disabled by pre-emption switchover. |
| CSCsl97653 | Cisco IOS | bcm2_5421_isr bcm2_num: 1 messages seen in the log |
| CSCsm01399 | Cisco IOS | Bus idle recovery may cause 10GE interface to remain down |
| CSCsm04824 | Cisco IOS | OER Top Talker Functionality broken on s3223 |
| CSCsm05486 | Cisco IOS | mtu mis probram in adj thru tunnel interface after b2b failover |
| CSCsm08419 | Cisco IOS | debounce timer issue on sup32 10GE uplink and 6708 |
| CSCsm11717 | Cisco IOS | VS2:On reloading standby chassis T/Bs on SP console for 1 minute |
| CSCsm13389 | Cisco IOS | RRI is not called be if QM rekey timer expiry forces SA deletion |
| CSCsm15350 | Cisco IOS | vpnspa crashed at assert failure in l2-mcpu.c on line |
| CSCsm20994 | Cisco IOS | kron job daily reoccurences fail after new year |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm21126 | Cisco IOS | C7600-SSC-400: Resync fabric interface on fabric error |
| CSCsm22935 | Cisco IOS | Problem in c6k_power_get_ilpower_daughterboard_used_pwr |
| CSCsm24904 | Cisco IOS | Bridge-mib timing out dot1dBasePortIfIndex |
| CSCsm26415 | Cisco IOS | Traceback seen when show platform cfm issued for fwd_vlan 0 |
| CSCsm27017 | Cisco IOS | VS2: power configuration is not synced to standby |
| CSCsm30858 | Cisco IOS | PIM register packets upmarked to TOS 6 by PTcam redirection |
| CSCsm32493 | Cisco IOS | Backout of CSCsh94882 |
| CSCsm33528 | Cisco IOS | Rekey packet loss for pure ipsec |
| CSCsm34871 | Cisco IOS | Need to support enhanced PoE feature |
| CSCsm35364 | Cisco IOS | SPA-IPSEC-2G get reload automatically by RP |
| CSCsm44309 | Cisco IOS | L2 Po - new member was not included in mapped ucast flood &mcast indices |
| CSCsm44413 | Cisco IOS | RP not added into LTL index when bridge-group is configured |
| CSCsm46682 | Cisco IOS | HL: VACL capture functionality not working with the latest sierra |
| CSCsm48564 | Cisco IOS | Need to exclude RxErrors from being monitored by LinkErrorMonitoring HM |
| CSCsm49103 | Cisco IOS | I/O Memory Leak when running show mls cef command |
| CSCsm49440 | Cisco IOS | RRI: Need to support remote-peer option when source proxy == peer |
| CSCsm51299 | Cisco IOS | Code divergence caused a need for a second fix for CSCsl27236. |
| CSCsm56293 | Cisco IOS | Sup4:DFC only mode, create bus stall condition-the switch still crash |
| CSCsm59488 | Cisco IOS | Fix backwards compatibility for multicast egress netflow cli |
| CSCsm70349 | Cisco IOS | BPDU traffic over Eompls is not switched on 3C system |
| CSCsm81399 | Cisco IOS | No Such Instance error from many SNMP objs for 1xOC48 POS/RPR SPA |
| CSCsm82169 | Cisco IOS | VSS: heathland interfaces are err-disabled on standby chassis |
| CSCsm82382 | Cisco IOS | 7600 standby RP memory leaking cause CEF disable |
| CSCsm83893 | Cisco IOS | W2: "sh mls cef adj mpls detai"l after SSO freeze RP causeT/B , reboot |
| CSCsm83948 | Cisco IOS | CISCO7609 returns sysObjectId as ciscoProducts.402 (which is cisco7606) |
| CSCsm92183 | Cisco IOS | c2w1: Heathland card is not coming up due to diag failure |
| CSCsm95456 | Cisco IOS | Duplicate L3 packets with 6708 and DEC |
| CSCsm96243 | Cisco IOS | Switch crashes on executing sh tcam interface acl with include option |
| CSCsm96610 | Cisco IOS | OOB-MAC-SYNC is on, need to change internally the cam aging to 480 Sec |
| CSCsm97836 | Cisco IOS | Memory leak VSL Manager |
| CSCsm98256 | Cisco IOS | Berytos got power down due to TestMacNotification and TestFabricCh0Healt |
| CSCso02208 | Cisco IOS | VS2: crash when provisioning LI stream |
| CSCso12903 | Cisco IOS | RE MET address check missing while running MET patch on IO bus timeout |
| CSCso25489 | Cisco IOS | CSCsg03804 - Time Based ACL Issue not fixed |
| CSCsl29993 | Content | WCCP Should Mark Client 'NOT Usable' with Missing L2 Adjacency |
| CSCsl65335 | Content | WCCP: reload following ACL update |
| CSCsm12247 | Content | WCCP: hash assignment may be lost after service group change |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm32473 | Content | WCCP: system reload with path splitting and output redirection |
| CSCsm35350 | Content | WCCP GRE return breaks IPsec traffic AND/OR creates phantom packet count |
| CSCsm53427 | Content | WCCP: multicast + appliance shutdown leads to high CPU |
| CSCsa57468 | Infrastructure | rttmon-mib does not return getnext value when queried via snmp |
| CSCse07265 | Infrastructure | No syslog message generated for IP SLA timeout condition |
| CSCsj54596 | Infrastructure | logging userinfo command no longer accepted |
| CSCsj83417 | Infrastructure | BOOM: addto_mempool_pc_array() message seen with show memory command |
| CSCsk06492 | Infrastructure | snmp-server drop vrf-traffic implementation in 12.2 SRB train |
| CSCsk13725 | Infrastructure | GSR: rttmon-mib does not return getnext value when queried via snmp |
| CSCsk37278 | Infrastructure | BFD clients flaps when boot string is removed from "show running" . |
| CSCsk75310 | Infrastructure | UDP Echo: control message not sent out of correct interface. |
| CSCsl33908 | Infrastructure | show ver truncates system's running image name to 64 chars |
| CSCsl58963 | Infrastructure | Manual OIR of pcmcia flash card crashes dosfs proc in Sup720 |
| CSCsl70722 | Infrastructure | Router crash polling rttmon mib with active IP SLA probes |
| CSCsg60447 | IPServices | 7200: BVI stops receiving CLNS/ISIS packets |
| CSCsi78892 | IPServices | Configuring bridge-group makes CPUHOG message. |
| CSCsj29841 | IPServices | Port forwarding breaks NAT-overload on a 6509 |
| CSCsj93195 | IPServices | RP crashes at ipv4fib_les_switch_wrapper on configuring crypto map |
| CSCsk06539 | IPServices | bus error while unconfiguring static SSM mappings via TFTP . |
| CSCsk39022 | IPServices | Modular IOS: ip directed-broadcast not working |
| CSCsk39926 | IPServices | Unable to route local FTP traffic over VRF with IOS image |
| CSCsl10348 | IPServices | Crash writing to or from ftp/tftp server in modular IOS |
| CSCsl23788 | IPServices | Dlsw+ peer waits in AB_PENDING or WAIT_WR status with modular IOS |
| CSCsk94676 | LegacyProtocols | dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH |
| CSCsk41552 | Management | T/B %SCHED-3-THRASHING of cdp2.iosproc process_wait_for_event |
| CSCsj34456 | MPLS | LDP change by CSCsi69278 causes inconsistent mplsLdpEntityIndex value . |
| CSCsk57114 | MPLS | CPUHOG process = SNMP ENGINE, PWMIB, GetNext of cpwVcMplsNonTeMappin |
| CSCsl39233 | MPLS | eBGP in VRF-lite not working in images without MPLS . |
| CSCsd14706 | Multicast | PIMV2 router send PIMV1 RP-reachable messages loading recieve router CPU |
| CSCsg95192 | Multicast | no ip rp-address <ACL name> causes an address error |
| CSCsj88725 | Multicast | Wrong (S,G) RPF after route change, no upstream join |
| CSCsl27840 | PPP | Router may Crash / Hang, Module Reset @ Shut ATM member + MLPOA |
| CSCsi73132 | QoS | Multicast DSCP value not copied to PIM-SM RP-register packet |
| CSCsk63794 | QoS | FlexWAN WS-X6582-2PA + T3+ Serial PA may crash/reload |
| CSCea90941 | Routing | IOS Ignores EIGRP Stub Command In Startup-Config at Initial Power On |
| CSCeg25475 | Routing | Distribute-list configured in ipv4 acts in vpnv4 address-family |
| CSCse53019 | Routing | redistribution not triggered when BGP as-path/community changes |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg80259 | Routing | BGP Routes do not re-populate follwing reload of Secodary Route Reflect |
| CSCsh12493 | Routing | BGP overlapping VRF route not installed in RIB after add/del of VRF |
| CSCsh92749 | Routing | ISIS: ADJ del triggers both LSP and SPF |
| CSCsi51431 | Routing | JQL:SIERRA:SP HighCPU/LCboot up fail with largeACL cfg after sw reload |
| CSCsk34344 | Routing | Wrong share-count 1:10 via confed-external BGP peers using dmzlink-bw |
| CSCsl07297 | Routing | SXF11: BGP "no neighbor" command caused Address Error exception . |
| CSCsl47915 | Routing | Redistribution of ospf in rip with prefix-list not working properly |
| CSCsl57457 | Routing | ISIS NSF switchover failure - similar to CSCsl28278 |
| CSCsl83415 | Routing | Rtr crash in show cmd: new updgrp add enlarges Nbr bitfield size for Tbl |
| CSCsl94410 | Routing | Back out the CSCsj17879 for all non ERF branch |
| CSCsm23764 | Routing | CEF RF progression error if RRP reloads mid CEF sync |
| CSCsm27979 | Routing | router may crash for "address error exception" doing sh ip route vrf |
| CSCsm64516 | Routing | OSPF MD5 Key Does Not Accept Whitespace Character |
| CSCso22098 | Routing | OSPF down on RPR+ switchover on core router |
| CSCin91851 | Security | Support keyboard-interactive authentication method |
| CSCsj45031 | Security | Cat6k unable to SCP files from Tectia ssh server |
| CSCsl98498 | Security | Tunnel int is going down with  mode ipip decapsulate-any |
| CSCsj68446 | WAN | NTP will not sync - NTP packets received but ignored by NTP process . |

## Caveats Resolved in Release 12.2(33)SXH1

### Resolved AAA Caveats

- CSCsj91123—Resolved in 12.2(33)SXH1

  **Symptoms:** Router reloads after authentication attempt fails on console.

  **Conditions:** Occurs while performing AAA accounting. The accounting structure was freed twice, which results in crash. Occurs when the **aaa accounting send stop-record authentication failure** command is configured, which sends a stop record for authentication failure.

  **Workaround:** Remove the **aaa accounting send stop-record authentication failure** command.

### Resolved Infrastructure Caveats

- CSCsk14633—Resolved in 12.2(33)SXH1

  This is the Cisco Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007 regarding the crash and reload of devices running Cisco IOS after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html

  The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html

Preliminary research pointed to a previously known issue that was documented as Cisco bug ID CSCsb08386 (registered customers only) , and entitled “PRP crash by show ip bgp regexp”, which was already resolved. Further research indicates that the current issue is a different but related vulnerability.

There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

The full text of this response is available at

http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070912-regexp

- CSCsk33054—Resolved in 12.2(33)SXH1

  This is the Cisco Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007 regarding the crash and reload of devices running Cisco IOS after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html

  The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html

  Preliminary research pointed to a previously known issue that was documented as Cisco bug ID CSCsb08386 (registered customers only) , and entitled “PRP crash by show ip bgp regexp”, which was already resolved. Further research indicates that the current issue is a different but related vulnerability.

  There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

  The full text of this response is available at

  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070912-regexp

- CSCsk61790—Resolved in 12.2(33)SXH1

  **Symptoms:** Syslog displays password when copying the configuration via FTP.

  **Conditions:** This symptom occurs when copying via FTP. The Syslog message displays the password given by the user as part of syntax of FTP copy.

  **Workaround:** There is no workaround.

#### Resolved Routing Caveats

- CSCsi84089—Resolved in 12.2(33)SXH1

  **Symptoms:** A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

  **Conditions:** This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

  **Workaround:** Add area 0 in the OSPF VRF processes.

  **Alternate Workaround:** Enter the **no capability transit** command in the OSPF VRF processes.

### Resolved Unknown Caveats

- CSCsi99869—Resolved in 12.2(33)SXH1

  **Symptom:** Bus error crash (signal 10) seen after the following error message:

  ```
  %MCAST-SP-6-GC_LIMIT_EXCEEDED: MLD snooping was trying to allocate more Layer 2
  entries than what allowed (7744)
  ```

  **Conditions:** This has been observed on a Catalyst6500 running IOS version 12.2(18)SXF1.

  **Workaround:** A workaround exist to disable ipv6 mld snooping via the command **no ipv6 mld snooping**.

  There is no negative impact of implementing the workaround as long as there is no IPV6 multicast traffic in the network.

### Other Resolved Caveats in Release 12.2(33)SXH1

| Identifier | Technology | Description |
|---|---|---|
| CSCek58496 | AAA | Mem alloc at aaa_test_setup_auth_req/aaa_test_setup_acct_req leaked |
| CSCsh59019 | AAA | Avoiding AAA client hangs, if a protocol subsystem is not present. |
| CSCsi99473 | AAA | TACACS authorization fails with 'request for nonexistent server' msg . |
| CSCsj34688 | AAA | AAA: adding static route cfg does not trigger acct msg to tacacs server |
| CSCsj89305 | AAA | RADIUS/NAS-IP address is sent out as 0.0.0.0 |
| CSCsj97165 | AAA | %AAA-3-BADMETHODERROR: Router crash @ aaa_get_new_acct_reg_type . |
| CSCsl33966 | AAA | C6509 : attribute 32 nas-Id not sent for Auth (missed by CSCsf30451 ) . |
| CSCsm06740 | AAA | Memory Leak in AAA accounting and Virtual Exec |
| CSCef67942 | Access | AS leaking memory under IP input - regcomp |
| CSCsi00099 | Access | Spurious Memory Access Error @ ct3sw_check_freedm_fifo |
| CSCsj37071 | Access | PA-MC-E3 will not recover after workload stress |
| CSCek61180 | ATM | crash @ write_to_url, doprintc_core, atm_remove_vc |
| CSCin90065 | ATM | ATM pvc trap may not always be generated or generated continously |
| CSCsb67229 | ATM | Ip add config on p2p interface tries to reflect it on all p2p int . |
| CSCse13374 | ATM | IMA ports on 7600 always initialized to default clocking on bootup . |
| CSCse98383 | ATM | Bandwidth not changed on IMA group when one member link is made down . |
| CSCsj57084 | ATM | Voice packets in LLQ experience latency |
| CSCdu70318 | Cisco IOS | Feature Request: VRF-lite PBR |
| CSCdz55178 | Cisco IOS | QoS profile name of more then 32 chars will crash the router . |
| CSCek34097 | Cisco IOS | with about 100 subints configd rtr crashes at ipv6 multicast-rout |
| CSCek36017 | Cisco IOS | Need show mac abbreviated equivalent command in IOS |
| CSCek52381 | Cisco IOS | Killing tcp.proc leads to no thread information in LC |
| CSCek75082 | Cisco IOS | Router crashes while unconfiguring channel-group |
| CSCek76062 | Cisco IOS | Router crashed @ validmem_complete_interrupt . |
| CSCek78066 | Cisco IOS | Whitney:CLI & MIB mismatch for aux-1 temperature Sensor SUP32 |
| CSCek78633 | Cisco IOS | SSO:ESM20:TB at %MFI-3-REDISTMGR: Redistribution Manager |

| Identifier | Technology | Description |
|---|---|---|
| CSCek79138 | Cisco IOS | VLAN policy not applied to bridged pkts if SVI shutdown . |
| CSCin99430 | Cisco IOS | snmp-server sparse is not working correctly for IF-MIB |
| CSCsa79984 | Cisco IOS | CTRLC_ENBL should be cleared when line is reset |
| CSCsb29131 | Cisco IOS | show crypto ipsec sa identity detail causes system to reload |
| CSCsc24830 | Cisco IOS | Far end router reload causing traceback at dmlp_update_hw_stats |
| CSCsc98471 | Cisco IOS | show diagnostic sanity  fails to check software modularity boot string . |
| CSCsd88768 | Cisco IOS | %SYS-2-BADSHARE: Bad refcount in datagram_done fix for PA-MCX-8TE1 |
| CSCse45684 | Cisco IOS | multicast (hsrp/ospf) coming from service modules is blackholed by vacl. |
| CSCse67736 | Cisco IOS | Add support for XFP-ZR optics |
| CSCsf01190 | Cisco IOS | Netflow export destination command dissapears from running config . |
| CSCsf97859 | Cisco IOS | invalid shows in show hw-module subslot with SPA-OC192POS-LR |
| CSCsg09423 | Cisco IOS | IPSEC SAs dont recover after rekey with 3000 IKE SAs and PKI (RSA-Sig) . |
| CSCsg15159 | Cisco IOS | Traffic to Null0 accounted with Null as dest IF |
| CSCsg16417 | Cisco IOS | show ip slb connections firewall cmd accepts not configured FW farm name |
| CSCsg19793 | Cisco IOS | Psecure absolute aging on DFC causes MAC  inconsistency w/ Central EARL |
| CSCsg21809 | Cisco IOS | Add bridge asic status collection support . |
| CSCsg23226 | Cisco IOS | service counters max age does not function correctly for value 6-9 sec |
| CSCsg29305 | Cisco IOS | hw-module subslot reload crashes the router . |
| CSCsg36532 | Cisco IOS | DMVPN Phase 2: Black hole traffic when spoke-spoke tunnel fails |
| CSCsg99914 | Cisco IOS | sip-200 power-cycles after BGP flap (not responding to keepalive) |
| CSCsh17579 | Cisco IOS | Transceiver TX Power displays erroneous TX level |
| CSCsh24450 | Cisco IOS | Memory leak from IF-MGR DB elem chunk @ im_if_db_init |
| CSCsh24460 | Cisco IOS | ipv6 ISIS ping through  doesnt return 100% success rate |
| CSCsh31782 | Cisco IOS | Bus error crash - show crypto isakmp sa |
| CSCsh34467 | Cisco IOS | Standby constanly reset due to RF request with large configuration . |
| CSCsh49239 | Cisco IOS | After redundancy failover Mcast packets drop for 60-90sec on SUP uplink |
| CSCsh64639 | Cisco IOS | VS2: [dead threads] process takes a large chunk of CPU util |
| CSCsh69341 | Cisco IOS | SLB: Incorrect feature execution in ssv |
| CSCsh80130 | Cisco IOS | Add warning/comments to interfaces when Auto Lag is used for interface |
| CSCsh82046 | Cisco IOS | SIERRA: sup4 standby crashes at sstrncpy during bootup. |
| CSCsh85531 | Cisco IOS | E1 channels down after PE reload |
| CSCsh88532 | Cisco IOS | Auto-LAG EtherChannel not configurable; doesn't trust QoS. . |
| CSCsh91974 | Cisco IOS | PIM CLI causes RP crash when issued under control-plane subconfig prompt |
| CSCsh97848 | Cisco IOS | Sierra: LACP pdus should be untagged . |
| CSCsh99583 | Cisco IOS | VTP's Local updater ID uses EOBC though up state SVIs exist |
| CSCsi00136 | Cisco IOS | IKE does not process more than 2 NAT-D payload |
| CSCsi05265 | Cisco IOS | SYS-2-GETBUF: Bad getbuffer -Process= LSDp Input Proc |

| Identifier | Technology | Description |
|---|---|---|
| CSCsi06759 | Cisco IOS | SIP 200: SNMP-3-DVR_DUP_REGN_ERR |
| CSCsi09942 | Cisco IOS | VTP3: Print warning message when the vlan name exceeds 20 characters |
| CSCsi11874 | Cisco IOS | Sup720 DFC forwarding some packets to MSFC instead of hw switching |
| CSCsi12416 | Cisco IOS | Native vlan traffic disruption in etherchannel standalone (I) mode |
| CSCsi23021 | Cisco IOS | WiSM in Slot 13 cause Duplicate IP message and loss of access |
| CSCsi24069 | Cisco IOS | Collect additional debug info for Modular IOS kernel crashes |
| CSCsi39631 | Cisco IOS | Show mpls l2transport vc detail using incorrect packet counters |
| CSCsi42270 | Cisco IOS | IOS-SLB Radius Server LB may not mark a real as failed |
| CSCsi48280 | Cisco IOS | PRE3 Mcast: Switchover not shown from default to data MDT |
| CSCsi49436 | Cisco IOS | Netflow API needs to be extended to provide peer AS information |
| CSCsi50028 | Cisco IOS | dot1x port moves authorize->guest, radius attributes and zombie MAC held |
| CSCsi65363 | Cisco IOS | Not able to run to t1 loopback when using a  PA-MC-T3 with flexwan |
| CSCsi70426 | Cisco IOS | Traceback seen when router received a craft EAP id-response frame |
| CSCsi71940 | Cisco IOS | System crashed with auto-qos negative test with traffic . |
| CSCsi74194 | Cisco IOS | 18SXF: Egress SPAN may cause high CPU |
| CSCsi76842 | Cisco IOS | Line protocol remains down on changing from frame-relay to hdlc/ppp. |
| CSCsi79991 | Cisco IOS | VACL capture not supported for the GE-WAN or GigabitEthernet on SIP-400 |
| CSCsi81885 | Cisco IOS | Trunk negotiation fails when Po is configured with Min_links . . |
| CSCsi82337 | Cisco IOS | Policy routing punts incoming packets to process with VRF select enabled |
| CSCsi87837 | Cisco IOS | IF-MIB does not support gig interfaces on  SPA-IPSEC-2G |
| CSCsi90816 | Cisco IOS | show policy-map interface caused sup32 crash . . |
| CSCsi91324 | Cisco IOS | MCAST packet drop when other interface goes down on DFC |
| CSCsi93273 | Cisco IOS | Leak in Big buffer pool on SIP card with NetFlow-export version 9 |
| CSCsi98587 | Cisco IOS | Excessive MET refs and memleak after ipv4 stress, crash follows . |
| CSCsi99234 | Cisco IOS | RP crash at validblock with %SYS-6-BLKINFO: Corrupted redzone blk |
| CSCsi99875 | Cisco IOS | BOOM: spa_eeprom_read_bit on BOOTUP |
| CSCsi99991 | Cisco IOS | When CMM is rebooted, FE goes into  ErrDisabled state |
| CSCsj00385 | Cisco IOS | logging event link-status default negates existing interface config |
| CSCsj01961 | Cisco IOS | ifindex table size from nvram sould be validated before malloc |
| CSCsj02971 | Cisco IOS | 12.2SRB - signed/unsigned error in code for 'show ip cache aggregation a |
| CSCsj03212 | Cisco IOS | blade get into bad b2b state if it is not b2b ready |
| CSCsj04905 | Cisco IOS | IOS-SLB: FWLB sticky config not get removed |
| CSCsj05519 | Cisco IOS | Standby NSE crashed IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP |
| CSCsj08713 | Cisco IOS | Disable bfd on SVI interfaces |
| CSCsj10375 | Cisco IOS | 802.1X: VLAN Changing on port causes link to go down |
| CSCsj10744 | Cisco IOS | Input queue wedged with Inband Edit Packets on SIP-400 |
| CSCsj11561 | Cisco IOS | Inconsistent MTU for Adj. entries used by MLS Netflow and MLS CEF |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj11771 | Cisco IOS | VS2: transceiver_rp_oir_online takes ~6s during reg_invoke_oir_online |
| CSCsj13444 | Cisco IOS | rsp720-10ge: PBR next-hop information lost on RPR switchover . |
| CSCsj14557 | Cisco IOS | Bogus Port channel 345 is created on simultaneous boot sometimes |
| CSCsj14847 | Cisco IOS | crypto connect command dropped after reload on unchannelized 2CT3+ . |
| CSCsj16292 | Cisco IOS | DATACORRUPTION-1-DATAINCONSISTENCY: copy error |
| CSCsj17048 | Cisco IOS | WS-X6708: show flow control shows send admin/oper state as desired |
| CSCsj17485 | Cisco IOS | Router crashed on doing a show cry isa pro while deleting them |
| CSCsj18494 | Cisco IOS | Leak +MN to pfc to avoid flooding due to tx span . |
| CSCsj27352 | Cisco IOS | RX Priority q-limit is set to default after reload |
| CSCsj28026 | Cisco IOS | WhitneyVS: Unable to mibwalk clcFdbVlanInfoTable . . |
| CSCsj28753 | Cisco IOS | IF-MIB::ifHCOutUcastPkts is incorrect on ESM20G |
| CSCsj29657 | Cisco IOS | Degradation in TPS - Whitney IOS image . |
| CSCsj32493 | Cisco IOS | IPSEC: Incorrect IPSec connection info in InvalidSPI testing |
| CSCsj34267 | Cisco IOS | SP crashes due to segmentation violation with 400 igmp groups/vrf |
| CSCsj34552 | Cisco IOS | ip address of vlan interface not programmed into spa-ipsec-2g |
| CSCsj35776 | Cisco IOS | Some of the VCs are INACTIVE after SPA OIR |
| CSCsj36689 | Cisco IOS | Corruption in block allocated by svclc_config |
| CSCsj38796 | Cisco IOS | LC/SP crash @ label_entry_get_inlabel |
| CSCsj42303 | Cisco IOS | 6K installs ffff.ffff.ffff in CAM table under very specific conditions |
| CSCsj48589 | Cisco IOS | BGP route (injected by OER) remains in Routing table after path is clear |
| CSCsj51666 | Cisco IOS | ip ssh ver 2 command missing in 12.2(25)EWA |
| CSCsj56703 | Cisco IOS | SSO failover causes RSTP forwarding and physical interfaces blocking . |
| CSCsj58538 | Cisco IOS | Lots of prowler/patriot interface go down for few second during sso swov |
| CSCsj61811 | Cisco IOS | process restart pcmcia_driver.proc on SP crashes the SP |
| CSCsj64453 | Cisco IOS | HSRP support in protocol policing |
| CSCsj66829 | Cisco IOS | Switch crash with clear ip igmp snoop stat and show ip igmp snoop st |
| CSCsj66987 | Cisco IOS | ifAlias for Subintf Reports the Previous Value if Description Deleted |
| CSCsj67096 | Cisco IOS | Issue w/NATed traffic on PortChannel (WS-X6408 and WS-X6516) on Sup720 |
| CSCsj72251 | Cisco IOS | BOOTP replies dropped if DHCP snooping is enabled |
| CSCsj72438 | Cisco IOS | Control plane instability and %EARL-DFC3-2-SWITCH_BUS_IDLE: Switching bu |
| CSCsj75636 | Cisco IOS | Crash in SP observed when per-port igmp statistics cleared |
| CSCsj77885 | Cisco IOS | %HA_EM-7-FMS_POLICY_MAX_ENTRIES message because of teminal length limit |
| CSCsj78751 | Cisco IOS | ES20: shut & no shut on ZR XFP causes the port to stay down |
| CSCsj80655 | Cisco IOS | timer value overflows when the specified val is larger than a long val |
| CSCsj81067 | Cisco IOS | IPSec VPN SPA: OLD-CISCO-CHASSIS-MIB does not return cardType |
| CSCsj81502 | Cisco IOS | show pagp clis are not displaying the correct information . |
| CSCsj83102 | Cisco IOS | crash upon card type configuration on WS-X6582-2PA / PA-MC-8TE1+ |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj84641 | Cisco IOS | some patches failed to commit during install commit of 41 patches. |
| CSCsj85930 | Cisco IOS | t/b  slot_earl_icc_shim_addr tm_send_message on changing to rpr |
| CSCsj86854 | Cisco IOS | SPAN does not  reset FPOE (to SP) when converting to distributed |
| CSCsj87584 | Cisco IOS | call-home inventory full needs show ipdrom switch all for VSS |
| CSCsj88208 | Cisco IOS | DOM not working for LR+ and ER+ Xenpaks |
| CSCsj88221 | Cisco IOS | class-default should not police BPDUs |
| CSCsj89470 | Cisco IOS | Bus Error crash in Netflow on 7200 running netflow and L2TP |
| CSCsj89905 | Cisco IOS | EEM applet hangs if system prompt is changed |
| CSCsj90252 | Cisco IOS | SYS-3-CPUHOG IP RIB Update seen on Active RP |
| CSCsj91795 | Cisco IOS | Appl TCs are not monitored when 12.2SRB BR is used with 12.4(15)T1 MC . |
| CSCsj95733 | Cisco IOS | Packet loss between sup4 uplink to 65xx modules |
| CSCsk02456 | Cisco IOS | TBs found @ pm_assert_fail. . |
| CSCsk02962 | Cisco IOS | Supervisor Reload after SSO switchover on Multicast MET reconstruction . |
| CSCsk03679 | Cisco IOS | VS2: show mls nde intermittently causes ALIGN-3-SPURIOUS T/B's |
| CSCsk06769 | Cisco IOS | shut on L2 int cause packets to loop back on T1 int causing traffic loss |
| CSCsk09155 | Cisco IOS | spa-ipsec-2g remains in Initialization state |
| CSCsk18206 | Cisco IOS | TCAM adjacency hardware programming problem with PBR and NAT . |
| CSCsk20346 | Cisco IOS | P router crash due to no EOBC buffer and illegal access to low address |
| CSCsk23521 | Cisco IOS | EARL-SPSTBY-2-SWITCH_BUS_IDLE is seen with SW switched traffic |
| CSCsk24272 | Cisco IOS | SUP720-3B  RP Crash due to I/O Buffer Leak by NDE w/ NAM 127.0.0.x Addr |
| CSCsk26973 | Cisco IOS | Memory leak in nhrp_cache_delete for incomplete cache entries |
| CSCsk30146 | Cisco IOS | Router crashed %DUMPER-3-PROCINFO: pid = 12315: (sbin/ios-base) SIGBUS |
| CSCsk33661 | Cisco IOS | show platform hardware capacity should include LTL usage . |
| CSCsk33724 | Cisco IOS | DOM does not work anymore for cwdm gbic/sfp |
| CSCsk33740 | Cisco IOS | replay window size of 1024 causes IPSec Policy Check and Replay Failure |
| CSCsk34237 | Cisco IOS | Egress multicast replication broken due to wccp . |
| CSCsk37675 | Cisco IOS | IKE stuck after several hours of IKE SA rekey . |
| CSCsk38024 | Cisco IOS | VS2: EtherChannel state on standby is incorrect due to out of order FEC |
| CSCsk41374 | Cisco IOS | device crash seen when auth-proxy enabled on the LPIP vlan . |
| CSCsk43058 | Cisco IOS | Port channel to WiSM controller suspended after upgrading to 12.2(33)SXH |
| CSCsk43673 | Cisco IOS | C2W1: Network RF client takes too long to process switchover . . |
| CSCsk45585 | Cisco IOS | Heathland: On bootup MPLS not supported on platform message |
| CSCsk55012 | Cisco IOS | setting portDuplex from 'full' to 'full'  may cause  standby reset . |
| CSCsk55423 | Cisco IOS | 7600's SPD implementation allow COS 5 or above in Extended headroom |
| CSCsk58810 | Cisco IOS | should NOT allow enable port-security on negotiating trunk interface . |
| CSCsk60874 | Cisco IOS | show tech needs 'show diagnostic results' and 'show diagnostic events' . |
| CSCsk60912 | Cisco IOS | MPLS forwarding table empty on standby RP . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsk62017 | Cisco IOS | multicast (hsrp/ospf) coming from service modules is blackholed by vacl. |
| CSCsk64860 | Cisco IOS | Config rollback to data file causes system to stuck at delete file mode. |
| CSCsk65482 | Cisco IOS | clear ip slb CLI is defined with wrong privilege level |
| CSCsk65860 | Cisco IOS | IOS-SLB:Security ACL breaks Client traffic |
| CSCsk67801 | Cisco IOS | WiSM:WiSM interfaces in manual LAG get shutdown at reload |
| CSCsk68656 | Cisco IOS | AB76: MFI push issu client msg type 5020 V1 MTU differ btwn SRB1/SRC |
| CSCsk70087 | Cisco IOS | Sup720 TLB exception created by fill_earl_vlan_stats_hdr . |
| CSCsk73627 | Cisco IOS | WS-X6548-GE-TX powered down due to keep alive polling feature |
| CSCsk78396 | Cisco IOS | Router may crash if SNMP walk on cefcModuleTable . |
| CSCsk80934 | Cisco IOS | Add errmsg to clearly indicate if lc reset due to power convertor failur |
| CSCsk82459 | Cisco IOS | VS2: continuous msg - Flooding detected in diag inband driver caused SSO |
| CSCsk82877 | Cisco IOS | METROPOLIS #0 cnt=1 reg:[1B0]kic_kic_int 02 |
| CSCsk83524 | Cisco IOS | L3 physical interface input drop counter is incorrect . |
| CSCsk83646 | Cisco IOS | BX10 ports don't link-up after Centaurus resets . . |
| CSCsk83683 | Cisco IOS | VRF-Lite aware PBR feature does not work after reload/SSO swover |
| CSCsk84944 | Cisco IOS | unidirectional Ethernet UDE is broken on WS-6704 after SW upgrade |
| CSCsk85987 | Cisco IOS | VS2: After 2 x SSO, SVI was down and multicast join didn't work |
| CSCsk86381 | Cisco IOS | KMI memory leak in 'IPSEC key engine' when delete p2 failed |
| CSCsk87262 | Cisco IOS | Switch crashes when polling port security MIB for SIP or Flexwan |
| CSCsk88173 | Cisco IOS | mac-address-table static with disable-snooping break on reboot |
| CSCsk88760 | Cisco IOS | 122SR:Routers crashes on unconfiguring vlan in the LACP mode |
| CSCsk89100 | Cisco IOS | 6196-RJ-21 Dropping all ingress frames with CRC counter incremented. |
| CSCsk89335 | Cisco IOS | After SSO switchover, see 6K DC power supplies mismatched . |
| CSCsk91267 | Cisco IOS | Module fails to come up with (FRU-power failed) |
| CSCsk93587 | Cisco IOS | TestFabricCh0Health test failure with unidir traffic via Ch1on Berytos |
| CSCsl04500 | Cisco IOS | OBFL process causing 6708 high CPU |
| CSCsl04687 | Cisco IOS | DFC3C pps counter does not work |
| CSCsl06110 | Cisco IOS | DHCP snooping agent: parse failures when importing the DB |
| CSCsl08912 | Cisco IOS | Vlan access list not working when have "xconnect vfi #" under the SVI |
| CSCsl13477 | Cisco IOS | SSO not working with crypto maps terminating at same peer address . |
| CSCsl23758 | Cisco IOS | WS-X6548-RJ-45: Wrong value of the output counter on show interface |
| CSCsl26981 | Cisco IOS | PBACL config causes hostname change when you downgrade to Rockies image |
| CSCsl26998 | Cisco IOS | Switch crashes on applying PBR with next-hop verify-availability |
| CSCsl41230 | Cisco IOS | IPSec SPA breaks IPSec if interesting traffic uses TCP ports |
| CSCsl70148 | Cisco IOS | PIM enabled p2p Crypto GRE Tunnels not installed in Hardware |
| CSCsl70634 | Cisco IOS | 67xx EC tx/rx traffic dependency resulting in low throughput |
| CSCsl94488 | Cisco IOS | Smartports CLI missing in sup32 ipbase image |

| Identifier | Technology | Description |
|---|---|---|
| CSCsm17983 | Cisco IOS | Memory corruption by  l3_mgr_e7_fmask_init_platform |
| CSCsi05906 | Content | WCCP:appliance failover does not update TCAM adjacency |
| CSCsi10700 | Content | WCCP:copy TOS value from inner to outer GRE packet |
| CSCsi91658 | Content | Wccp stops layer 2 redirection when dscp is present in the redirect acl |
| CSCsj09149 | Content | WCCP: no redirection following change in configuration |
| CSCsj48440 | Content | WCCP: L2 return traffic is software switched |
| CSCsk14208 | Content | WCCP does not work after OIR or Reboot |
| CSCsl04908 | Content | WCCP: shutdown of appliance i/f leads to c6k reload |
| CSCsb95806 | Infrastructure | Incorrect 64bit counter on 1Gb MPLS interface via SNMP . |
| CSCsc33389 | Infrastructure | When snmp-server host is deleted, the trap is not sent to other hosts |
| CSCsc84077 | Infrastructure | IOS CLI will stop accepting octal by default |
| CSCsd52019 | Infrastructure | cieIfStateChangeReason and locIfReason support broken. |
| CSCsf30779 | Infrastructure | Add CLI for section keyword in show run output modifiers |
| CSCsh25151 | Infrastructure | memory leak seen with reflexive ACL and NAT/PAT |
| CSCsh48919 | Infrastructure | Embedded spaces in DOSFS dirs/file names cause crash in some platforms |
| CSCsh81291 | Infrastructure | Exodus Mayflower C10K ISSU fails at loadversion |
| CSCsj37635 | Infrastructure | Incorrect source IP address is used for IP SLA icmp-echo with VRF |
| CSCsj58223 | Infrastructure | Bus Error after 'show memory' . |
| CSCsj80951 | Infrastructure | *Neutrino*  proc reported memory  Freed/Holding is incorrect |
| CSCsj83924 | Infrastructure | Porting command show history all to mainlines |
| CSCsj83966 | Infrastructure | Syslog traps cause CPUHOG when lot of interface come up at same time. . |
| CSCsk10335 | Infrastructure | Traceback @ ipc_send_message_blocked during bootup . |
| CSCsk27147 | Infrastructure | SNMP stops responding while polling from CISCO-MEMORYPOOL-MIB |
| CSCsk38461 | Infrastructure | Show platform hardware command getting rejected . |
| CSCsk67272 | Infrastructure | CPU HOG while polling ciscoFrameRelayMIB . |
| CSCsl09867 | Infrastructure | Exec-timeout not working at more prompt when using Modular IOS |
| CSCsl13216 | Infrastructure | warm upgrade is not working . |
| CSCsl53110 | Infrastructure | VSS: Stby rp crashes on boot |
| CSCeh56158 | IPServices | NAT outside source translation fails for GRE packets . |
| CSCsg97662 | IPServices | Cant disable skinny (tcp 2000) . |
| CSCsh92986 | IPServices | Very long latency for RSH traffic going through FWSM . |
| CSCsi16903 | IPServices | IGMPv3 mode 4 group report with {} source list gets translated to mode 6 |
| CSCsi28444 | IPServices | DHCP server has parse problems with x in bootfile |
| CSCsi42717 | IPServices | saa_vrf_test_udpe & saa_vrf_test_itter generate an unexpected error mess |
| CSCsi57927 | IPServices | FTP session hangs TCP in closewait after CLI times out . . |
| CSCsj07951 | IPServices | Memory Corruption when Autoinstall over FR |
| CSCsj62846 | IPServices | Need to differentiate IPv4 and IPv6 . . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj89544 | IPServices | TCP retransmissions get dropped below IP layer. . |
| CSCsk07170 | IPServices | MD5 validation error shows IPv4 address but should IPv6 address |
| CSCsk10604 | IPServices | Syn pkts destined to VRF fail to match the default TCB in table |
| CSCsk29013 | IPServices | IGMP groups in the vrf not rejoined after executing a cle ip mr vrf |
| CSCsk80935 | IPServices | SXF12, SNMP response being broadcast . |
| CSCsk81396 | IPServices | NAM process crash in 12.2SXF . |
| CSCsk82821 | IPServices | The UUT not able to receive the Large ICMP message. |
| CSCsl00350 | IPServices | ARP entry not created for nat translated IP . |
| CSCsl06431 | IPServices | Modular IOS: Memory leak in udp.proc |
| CSCsc77148 | LegacyProtocols | Router crash while issuing show ipx cache command. Cleanup SA warnings. |
| CSCsh34949 | LegacyProtocols | DLSW router crash with Bus Error |
| CSCsj98895 | LegacyProtocols | v2-single-tcp peer connection is  established on a  non confg/prom peer |
| CSCsg05873 | Management | Buffer leak with SNA Focalpoint PU consuming middle buffers with NMVTs |
| CSCsk36618 | Management | Device crash with cdp traffic @ 200 pkts/sec and clear cdp table |
| CSCsi75566 | MPLS | Packets dropped on FRR backup tunnel if protected intf is dot1q |
| CSCsi99825 | MPLS | 7613 crashed on SNMP ENgine |
| CSCsj55865 | MPLS | Traceback seen @ lsd_rewrite_create and lsd_frr_co_req |
| CSCsk14113 | MPLS | LDP change in advertise-tag for access list stop advertising some prefix |
| CSCsk57589 | MPLS | TB:%LFD-3-INVINSTALLER & %BGP_MPLS-3-VPN_REWRITE(seen on bootup) |
| CSCec55244 | Multicast | PIMv6: Spurious access at pim_ipv6_hello_addr_adv_size |
| CSCek26940 | Multicast | Need to unhide interval for send-rp-discovery |
| CSCsh56720 | Multicast | CPUHOG/Watchdog timeout when using igmp static group class-map cmd |
| CSCsi01481 | Multicast | %PIM_PROT-3-SHUTDOWN_ERR seen at unconfig ipv6 pim rp-addr . |
| CSCsi97586 | Multicast | MGX-RPM-XF-512 reset after customer deleted multicast vpn and vpn vrf |
| CSCsj16861 | Multicast | Dynamically overwritten bidir RP doesn't get removed from HW |
| CSCsj64230 | Multicast | bidir DF election should not be restarted on a downstream interface |
| CSCsk49073 | Multicast | %DUMPER-3-PROCINFO ... SIGSEGV when running Extranet MVPN |
| CSCef54653 | PPP | Members inactive in a multilink bundle except the first member. . |
| CSCse28421 | PPP | %AAAA-3-BADSTR error when Multilink interface goes down . |
| CSCek49107 | QoS | Router crashes @ traffic_shape_dequeue_shim . |
| CSCek78675 | QoS | SIP200 crash at hqf_cwpa_pak_enqueue_local during qos test . |
| CSCse18146 | QoS | SIP1-CT3: SIP1 crashed after switchover @giant_node_process . |
| CSCsg98040 | QoS | QoS applied to int with dot1q trunk does not match MPLS EXP on 12.2S |
| CSCsk09651 | QoS | Router may reload with shaping policy on MLPPPoFR . . |
| CSCec43841 | Routing | EIGRP: IP next-hop incorrect on spokes when using no next-hop-self |
| CSCek33384 | Routing | Tunnels stay down after cutover at MPLS head test cases |
| CSCek75079 | Routing | Problem in type7 to type5 translation if summary-addr configured |

| Identifier | Technology | Description |
|---|---|---|
| CSCek76776 | Routing | ip interface settings persistent after deleting/adding sub-interface |
| CSCek78315 | Routing | Access to NULL ptr with debug ip ospf hello . |
| CSCek79264 | Routing | static route tracked by track-object not installed into routing tabl . |
| CSCsa73179 | Routing | Memory corruption/crash when 'no default-information orig' under RIP |
| CSCsc73725 | Routing | EIGRP packet pacing should have lower minimum value |
| CSCsd34114 | Routing | IPv6 Localpools allows more than one prefix per user |
| CSCse42362 | Routing | EIGRP next hop not updated on spoke, in a dual hub/dual path dmvpn topo |
| CSCsf27220 | Routing | Router crashes on traffic with NHRP |
| CSCsg12385 | Routing | No IPv6 uRPF subblock control decode function |
| CSCsg16778 | Routing | router may crash at  bgp_update_nbrsoo after deleting BGP neighbor . |
| CSCsg25995 | Routing | N/w configured are not seen  in mbgp table with nbr nlri unicast multi |
| CSCsg63932 | Routing | IPv6 Static issue with same path from two clients |
| CSCsg72029 | Routing | setting M bit in RA supresses autoconfig bit |
| CSCsg94088 | Routing | OSPF route map not matching community-list / ipv6 redistributing bgp |
| CSCsh20656 | Routing | TCP header compression elicits upstream retransmissions from Fritz |
| CSCsh38140 | Routing | CEF drops when using CEF LB paths and active link recovers from failure |
| CSCsh54797 | Routing | high CPU in collection process after bringing up pppoe sessions twice . |
| CSCsh57509 | Routing | RIPv2 does not delete redundant paths with different next hops . |
| CSCsh80008 | Routing | BGP: soft reconfiguration inbound and neighbor weight has no effect |
| CSCsh82953 | Routing | EIGRP pece routes missing extcomm attrs after redistribution to BGP . |
| CSCsh87744 | Routing | IPv6 mcast: RPF fails even while MBGP has default route |
| CSCsh88825 | Routing | bgp: advertisement-interval not nvgened for peer-groups |
| CSCsi09698 | Routing | BGP adv connected prefixes suppressed by IP Event Dampening after reload |
| CSCsi15183 | Routing | change MTU value causes  %DUAL-3-INTERNAL in ipigrp2_add_item_dest |
| CSCsi17002 | Routing | IPv6 PBR policy routes to non-attached destination |
| CSCsi25729 | Routing | ISIS doesn't enable BFD except after micro reload |
| CSCsi27696 | Routing | oldest ebgp bestpath not retained in eibgp multpath cases |
| CSCsi33147 | Routing | OSPFv3: prefix lsa does not re-originate after interface comes up . |
| CSCsi41109 | Routing | Traffic loss and High RP CPU with SPA OIR with a large configuration |
| CSCsi47635 | Routing | deleted sub-interface shows up on next config sub-interface |
| CSCsi48304 | Routing | Multi-source redistributing makes ospfv3 external db corrupt |
| CSCsi53353 | Routing | BGP TTL Hack breaks ipv6 neighbor |
| CSCsi58303 | Routing | eigrp resync peer graceful-restart repeatedly after reload . |
| CSCsi58867 | Routing | CPUHOG After show ip route static or show ip route connected |
| CSCsi62017 | Routing | %XDR-DFC3-6-XDRLCDISABLEREQUEST: Client XDR Interrupt Priority Client |
| CSCsi80057 | Routing | RIP default-information originate with route-map not working correctly . |
| CSCsj00161 | Routing | IPv6 may load balance between summary discard and reachability paths . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj04761 | Routing | No space between 'any' and 'eq' after configuring ipv6 acl |
| CSCsj06265 | Routing | Switch crashes when doing clear ip ospf process |
| CSCsj09838 | Routing | RR some prefix might not be sent after bgp neighbor flaps . |
| CSCsj10185 | Routing | CPU hog in ospfv3_clean_partial_spfQ and ospf_clean_partial_spfQ |
| CSCsj17820 | Routing | Hub crashes during unconfiguration due to program counter error |
| CSCsj17950 | Routing | ISIS redistributed static routes might not be advertised |
| CSCsj25841 | Routing | default not sent using neighbor default-originate conditionally w/route |
| CSCsj25940 | Routing | %SYS-2-NOTQ: unqueue didn't find 6433F698 in queue . |
| CSCsj32013 | Routing | GSR crashing with bgp_vpnv4_purge_one_import . |
| CSCsj36133 | Routing | Invalid header length BGP notification when sending withdraw |
| CSCsj37111 | Routing | IPv4 inconsistencies & %FIB-4-FIBXDRINV upon reset LC |
| CSCsj53361 | Routing | ISIS flaps after NSF/SSO of peer with 16 neighbor,5k routes and traffic. |
| CSCsj54395 | Routing | router crash when iphc configured with SLIP encap |
| CSCsj64154 | Routing | c7600 - %SIP200_MP-4-PAUSE: Non-master CPU is suspended for too long |
| CSCsj71306 | Routing | mfibv4: HA: BGP MDT update is injected into standby . . |
| CSCsj72039 | Routing | Prefix not in ISIS database if serial interface and passive |
| CSCsj80615 | Routing | BGP not sending prefix with expected next hop to the peers . . |
| CSCsj85485 | Routing | EIGRP NSF - MSFC switchover causes hello's to be sent over passive intf |
| CSCsj89636 | Routing | isis convergance time delay with equal paths |
| CSCsj97484 | Routing | 32kEVC: ESM LC OIR crash causes RP to crash when LC comes up. |
| CSCsj99269 | Routing | BGP: VPNv4 general scanner runtime close to 1 hour at boot time . |
| CSCsk21328 | Routing | 6504 crashes in IPV6 |
| CSCsk26719 | Routing | show ip access crash with per-user acl |
| CSCsk27077 | Routing | router crash observed while clearing  virtual access interface |
| CSCsk29853 | Routing | ospf takes almost 10 minutes to flash Stale, self-originated LSAs |
| CSCsk33115 | Routing | OSPF virtual-link fails to come up during IETF GR & RIB entries deleted |
| CSCsk35970 | Routing | BGP Router/Scanner causes high CPU utilization when using BGP multipath |
| CSCsk35985 | Routing | OSPFv3: router crashes for "show ipv6 ospf lsdb" after redist of routes |
| CSCsk36324 | Routing | OSPF: spf calculation goes into loop causing high CPU . |
| CSCsk38877 | Routing | PE_PUNT_UNRECOGNIZED should be an OUTPUT_FEATURE . |
| CSCsk46195 | Routing | Arp entry does not age out with private vlans and no ip sticky-arp |
| CSCsk48182 | Routing | BGP: Router crashes @ bgp_netlist_validate |
| CSCsk66339 | Routing | ISIS fails remove native path from local RIB /  del path from global RIB |
| CSCsk89546 | Routing | RIB and FIB not updated after shut TE LB path |
| CSCsl13950 | Routing | VS2:XDR_LC traceback seen on Standby-RP on bootup . |
| CSCsl18176 | Routing | OSPF SPF calculation with TE metric absolute picks wrong egress . |
| CSCsl28278 | Routing | OSPF-Route/CEF entry lost after SSO on the neighbor |

| Identifier | Technology | Description |
|---|---|---|
| CSCsl71540 | Routing | Router crash after using cmd 'sh ip bgp x.x.x.x [bestpath |
| CSCsh72664 | Security | DMVPN: OSPF neighbor flap and traceback @ tunnel_oqueue. . |
| CSCsj60938 | Security | SCP with redirect option locks up console or VTY line . |
| CSCsj78065 | Security | tunnel_trace CPUHOG in Net Background process |
| CSCsk00054 | Security | mGRE fragmentation into tunnel broken |
| CSCei22295 | WAN | Traceback is seen at fr_svc_teardown_calls |
| CSCsc38968 | WAN | Frame-relay EEK failure does not keep subinterface down |
| CSCsi70599 | WAN | Standby reloads due to Config Sync: Line-by-Line sync verifying failure |

## Caveats Resolved in Release 12.2(33)SXH

### Resolved AAA Caveats

- CSCsg88561—Resolved in 12.2(33)SXH

  **Symptom:** When accessing VTY lines configured for TACACS AAA authentication, the remote access session will not get access to the device.

  **Conditions:** If using TACACS for VTY user authentication the remote access session will stop being processed after the username and password have been entered. Operation of the device continues as per normal, just the remote VTY session can not be used.

  Limited to C7600 ONLY.

  **Workaround:** Local Authentication or RADIUS could be used as a workaround.

### Resolved Content Caveats

- CSCsi46028—Resolved in 12.2(33)SXH

  **Symptom:** On routers that are configured for WCCP, interfaces that are connected to the content engine can become locked. By locked what is meant is that the interface driver is in a state where the physical interface will stop sending and receiving packets.

  **Conditions:** This issue has been introduced by CSCuk61396, only the images that have the fix for CSCuk61396 are affected by this issue.

  **Workaround:** There are no workarounds. If an interface becomes locked, the only way to recover the system is to do a reload.

### Resolved Infrastructure Caveats

- CSCsc64976—Resolved in 12.2(33)SXH

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20051201-http.html

- CSCsi13344—Resolved in 12.2(33)SXH

  **Symptom:** Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http

  **Conditions:** See “Additional Information” section in the posted response for further details.

  **Workarounds:** See “Workaround” section in the posted response for further details.

- CSCsf04754—Resolved in 12.2(33)SXH

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of

network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

This advisory will be posted at

http://www.cisco.com/en/US/products/csa/cisco-sa-20080610-snmpv3.html

#### Resolved IPServices Caveats

- CSCsh04686—Resolved in 12.2(33)SXH

  **Symptoms:** With X.25 over TCP (XOT) enabled on a router or Catalyst switch, malformed traffic that is sent to TCP port 1998 causes the device to reload. This symptom was first observed in Cisco IOS Release 12.2(31)SB2.

  **Conditions:** This symptom is observed only when X.25 routing is enabled on the device.

  **Workaround:** Use IPsec or other tunneling mechanisms to protect XOT traffic. Also, apply ACLs on affected devices so that traffic is accepted only from trusted tunnel endpoints.

- CSCsi39674—Resolved in 12.2(33)SXH

  **Symptom:** Devices may reload upon receiving multiple short lived TCP sessions to the telnet port.

  **Conditions:** Devices that run IOS and support IOS Software Modularity are affected. Images that support IOS Software Modularity will have “-vz” in their image name.

- CSCse56501—Resolved in 12.2(33)SXH

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6

- CSCek37177—Resolved in 12.2(33)SXH

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177

There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-crafted-tcp.html

#### Resolved LAN Caveats

- CSCsd34759—Resolved in 12.2(33)SXH

  **Symptom:** The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  **Conditions:** The packets must be received on a trunk enabled port.

  **Further Information**

  On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759 -- VTP version field DoS
  - CSCse40078/CSCse47765 -- Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611 -- Buffer Overflow in VTP VLAN name

  Cisco's statement and further information are available on the Cisco public website at

  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20060913-vtp

#### Resolved LegacyProtocols Caveats

- CSCsf28840—Resolved in 12.2(33)SXH

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070110-dlsw.html

#### Resolved Management Caveats

- CSCsf07847—Resolved in 12.2(33)SXH

  **Symptoms:** Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  **Conditions:** This issue occurs in IOS images that has the fix for CSCse85200.

  **Workaround:** Disable CDP on interfaces where CDP is not required.

  **Further Problem Description:** Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

### Resolved MPLS Caveats

- CSCsa52940—Resolved in 12.2(33)SXH

  **Symptoms:** A Cisco HE router running MPLS traffic engineering may crash with a memory corruption footprint or with a bus error. If the P and PE routers are running a release prior to 12.0(26)S or 12.2S Cascades, then all of the downstream midpoint routers may crash with similar symptoms.

  **Conditions:** More than 10 LSPs for a single MPLS-TE session must be signalled in a specific way, which is not supported nor used by Cisco IOS.

  Multiple LSPs for a single session will only happen when the router is under great stress because of many tunnels or breakage somewhere else in the network.

  Note that this is not a problem when MPLS-TE tunnels are signalled with verbatim LSPs, because Cisco routers signal verbatim LSPs do not use this type of signalling.

  **Workaround:** None

### Resolved Multicast Caveats

- CSCse15770—Resolved in 12.2(33)SXH

  **Symptom:** IOS device may reload unexpectedly

  **Conditions:** The Multicast Routing Monitor (MRM) feature must be enabled and corrupted traffic is received by the MRM responder.

  **Workarounds:** Disable the MRM feature,

### Resolved Routing Caveats

- CSCec12299—Resolved in 12.2(33)SXH

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn

- CSCed40933—Resolved in 12.2(33)SXH

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory which is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-ipv6.

- CSCef67682—Resolved in 12.2(33)SXH

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

  The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

  This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognises as its own.

  This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

  We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html contain fixes for this issue.

- CSCsd58381—Resolved in 12.2(33)SXH

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html

#### Resolved Security Caveats

- CSCsg40567—Resolved in 12.2(33)SXH

  **Symptoms:** Malformed SSL packets may cause a router to leak multiple memory blocks.

  **Conditions:** This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

  **Workaround:** Disable the **ip http secure server** command.

- CSCsc19259—Resolved in 12.2(33)SXH

  The server side of the Secure Copy (SCP) implementation in Cisco Internetwork Operating System (IOS) contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS Secure Copy Server service are not affected by this vulnerability.

This vulnerability does not apply to the IOS Secure Copy Client feature.

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-scp.html.

- CSCse50135—Resolved in 12.2(33)SXH

  **Symptom:** Using scripts to access a Cisco IOS device may bypass the command authorization feature.

  **Conditions:** AAA is configured

  **Workarounds:** None

- CSCsd85587—Resolved in 12.2(33)SXH

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM) CSCsi97695

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-crypto.html .

  **Note:** Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-SSL.html

- CSCse24889—Resolved in 12.2(33)SXH

  **Symptoms:** Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  **Conditions:** This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

**Workaround:** As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t
ip ssh version 1 end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that is permitted access to the router, all other
access is denied
access-list 99 permit 10.1.1.0 0.0.0.255 access-list 99 deny any
line vty 0 4 access-class 99 in end
```

**Further Problem Description:** For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cntrl_acc_vtl.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

### Resolved Unknown Caveats

- CSCek49649—Resolved in 12.2(33)SXH

  **Symptoms:** Cisco Catalyst 6500 and Cisco 7600 modules are reachable via 127.0.0.x addresses.

  **Conditions:** Cisco Catalyst 6500 and Cisco 7600 series devices use addresses from the 127.0.0.0/8 (loopback) range in the Ethernet Out-of-Band Channel (EOBC) for internal communication.

  Addresses from this range that are used in the EOBC on Cisco Catalyst 6500 and Cisco 7600 series devices are accessible from outside of the system. The Supervisor module, Multilayer Switch Feature Card (MSFC), or any other intelligent module may receive and process packets that are destined for the 127.0.0.0/8 network. An attacker can exploit this behavior to bypass existing access control lists; however, an exploit will not allow an attacker to bypass authentication or authorization. Valid authentication credentials are still required to access the module in question.

  Per RFC 3330, a packet that is sent to an address anywhere within the 127.0.0.0/8 address range should loop back inside the host and should never reach the physical network. However, some host implementations send packets to addresses in the 127.0.0.0/8 range outside their Network Interface Card (NIC) and to the network. Certain implementations that normally do not send packets to addresses in the 127.0.0.0/8 range may also be configured to do so..

  Destination addresses in the 127.0.0.0/8 range are not routed on the Internet. This factor limits the exposure of this issue.

  This issue is applicable to systems that run Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the MSFC) and Native Mode (IOS Software on both the Supervisor Engine and the MSFC).

  **Workaround:** Administrators can apply an access control list that filters packets to the 127.0.0.0/8 address range to interfaces where attacks may be launched.

  ```
  ip access-list extended block_loopback
    deny   ip any 127.0.0.0 0.255.255.255
    permit ip any any
  ```

```
interface Vlan x
 ip access-group block_loopback in
```

Control Plane Policing (CoPP) can be used to block traffic with a destination IP address in the 127.0.0.0/8 address range sent to the device. Cisco IOS Software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks. CoPP protects the management and control planes by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

```
!-- Permit all traffic with a destination IP
!-- addresses in the 127.0.0.0/8 address range sent to
!-- the affected device so that it will be policed and
!-- dropped by the CoPP feature
!
access-list 111 permit icmp any 127.0.0.0 0.255.255.255
access-list 111 permit udp any 127.0.0.0 0.255.255.255
access-list 111 permit tcp any 127.0.0.0 0.255.255.255
access-list 111 permit ip any 127.0.0.0 0.255.255.255
!
!-- Permit (Police or Drop)/Deny (Allow) all other Layer3
!-- and Layer4 traffic in accordance with existing security
!-- policies and configurations for traffic that is authorized
!-- to be sent to infrastructure devices
!
!-- Create a Class-Map for traffic to be policed by the
!-- CoPP feature
!
class-map match-all drop-127/8-netblock-class
  match access-group 111
!
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
!
policy-map drop-127/8-netblock-traffic
  class drop-127/8-netblock-class
    police 32000 1500 1500 conform-action drop exceed-action drop
!
!-- Apply the Policy-Map to the Control-Plane of the
!-- device
!
control-plane
  service-policy input drop-127/8-netblock-traffic
!
```

Additional information on the configuration and use of the CoPP feature is available at the following links:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

Infrastructure Access Control Lists (iACLs) are also considered a network security best practice and should be considered as, long-term additions to effective network security as well as a workaround for this specific issue. The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection ACLs. The white paper is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

- CSCsd68605—Resolved in 12.2(33)SXH

  **Symptoms:** If a spoke cannot complete IKE phase I because of a bad certificate, the failed IKE sessions may not be deleted on an IPSec/IKE responder. Such failed sessions may accumulate, eventually causing router instability. These failed sessions can be seen in the output of the **show crypto isakmp sa | i MM** command:

```
172.18.95.21    10.253.34.80   MM_KEY_EXCH        898    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        896    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        895    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        894    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        893    0 ACTIVE
...
```

  **Conditions:** These symptoms are observed when RSA signatures are used as the authentication method.

- CSCsd75273—Resolved in 12.2(33)SXH

  Cisco Catalyst 6500, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

- CSCsf12082—Resolved in 12.2(33)SXH

  Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

  OSPF and MPLS VPNs are not enabled by default.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue

- CSCsg53589—Resolved in 12.2(33)SXH

  **Symptom:** On c7600 router with DHCP Relay agent configured on unnumbered Vlan interface, DHCP packets (DHCP ACK / DHCP OFFER), comming from the DHCP server, can be padded with random bits of data and packet lenght field is not updated.ng too.

  **Conditions:** DHCP Relay is configured on Vlan interface with “ip helper address”

  **Workaround:** Disable DHCP Snooping

- CSCsi01470—Resolved in 12.2(33)SXH

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html.

- CSCsi86396—Resolved in 12.2(33)SXH

  **Symptoms:** Two subinterfaces may have the same CEF interface index.

  **Conditions:** This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when the following configuration sequence occurs:

  1) Create subinterface 1, 2, and 3.

  2) Delete subinterface 1.

  3) Create subinterface 4.

  4) Enable subinterface 1.

  In this situation, subinterface 1 and 4 may have the same CEF IDB.

  **Workaround:** There is no workaround. You must reload the platform to clear the symptoms.

- CSCsi99869—Resolved in 12.2(33)SXH

  **Symptom:** Bus error crash (signal 10) seen after the following error message:

  ```
  %MCAST-SP-6-GC_LIMIT_EXCEEDED: MLD snooping was trying to allocate more Layer 2
  entries than what allowed (7744)
  ```

  **Conditions:** This has been observed on a Catalyst6500 running IOS version 12.2(18)SXF1.

  **Workaround:** A workaround exist to disable ipv6 mld snooping via the command **no ipv6 mld snooping**.

  There is no negative impact of implementing the workaround as long as there is no IPV6 multicast traffic in the network.

- CSCsj16969—Resolved in 12.2(33)SXH

  **Symptom:** A Cisco IOS device supporting IPv6 MLD may crash with a data bus error exception and stack trace PC = 0xA0000100

  **Conditions:** Device is running normal production traffic. Presence of malformed MLD packet in this network caused the issue.

  **Workaround:** Disabling MLD snooping on the VLAN or globally on the box will stop the crash.

- CSCek36513—Resolved in 12.2(33)SXH

  **Symptom:** When allocating buffers for the initial creation of a Crypto Key an error may occur that could cause the Crypto engine to generate an incorrectly sized key.

  **Conditions:** None

  **Workaround:** None

- CSCse52951—Resolved in 12.2(33)SXH

  Cisco Catalyst 6500, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

- CSCsh73972—Resolved in 12.2(33)SXH

  **Symptom:** Unicast traffic originating from a SPA card may not be encrypted

  **Condition:** Traffic originates from a SPA card in a SIP-600. Outbound traffic is configured for GRE with tunnel protection.

  **Workaround:** None

- CSCsg70474—Resolved in 12.2(33)SXH

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

#### Resolved Voice Caveats

- CSCsd81407—Resolved in 12.2(33)SXH

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

- CSCsc60249—Resolved in 12.2(33)SXH

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

- CSCsi60004—Resolved in 12.2(33)SXH

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

- CSCeb21064—Resolved in 12.2(33)SXH

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

### Other Resolved Caveats in Release 12.2(33)SXH

| Identifier | Technology | Description |
|---|---|---|
| CSCdp33836 | AAA | unhide aaa authorization console and warn user |
| CSCef27578 | AAA | The router crashes when test aaa stop CLI is issued |
| CSCek46627 | AAA | Accounting method list update failed . |
| CSCsa40461 | AAA | VRF-aware TACACS+ not working with enable authentication |
| CSCsb11698 | AAA | Input Queue Wedge with TACACs |
| CSCsd49317 | AAA | no tacacs-server administration causes router hang . |
| CSCsd71301 | AAA | Depending on Attriubut order send from aaa server priv level assigned. |
| CSCsd95752 | AAA | 6500 TACACS message sent to wrong server . |
| CSCse45735 | AAA | %AAAA-3-NOREG: authentication method 5 has no registry! T/B |
| CSCse69002 | AAA | Accounting of auth failure doesn't work with some switches |
| CSCsf30451 | AAA | radius-server attrib 32 include-in-access-req/accounting-req not sent |
| CSCsg43322 | AAA | AAA: No free authorization/accounting lists for network |
| CSCsh23142 | AAA | aaa local authentication not happening for authproxy . |
| CSCsh43536 | AAA | aaa group server config lost after reboot |
| CSCsh46990 | AAA | Console hangs with enable/line as aaa fall-back methods |
| CSCef35417 | Access | 7200:Frame-relay LMI messages are not being handled correctly |
| CSCef81197 | Access | Rx-error throttling disabled on VIP after OIR |
| CSCeg55131 | Access | Spurious access @mip_unchain_idb while configuring t1 controller |
| CSCeh01287 | Access | FR/WAN over IP: Required sessions are not establised. keeps flaping |
| CSCei05246 | Access | CE3 interface output frozen after OIR VIP6-80 |

| Identifier | Technology | Description |
|---|---|---|
| CSCin88048 | Access | unchannelized interface line -protocol not coming up |
| CSCsa64102 | Access | Spurious accesses and Badshare with PA-MC-T3 |
| CSCsa83881 | Access | PA-T3+: interface port remains up during unavailable seconds |
| CSCsa83897 | Access | PA-MC-T3: T3 port does not enter UAS during high P and C-bit error rates |
| CSCsa93523 | Access | 7200 PA-E3 incrementing carrier transitions and packet drops |
| CSCsb07696 | Access | HYPERION-4-HYP_RESET: Hyperion Error Interrupt |
| CSCsb21867 | Access | PA-MC-8TE1+ in Flexwan: ctrlr detects LOS after restart does not recover |
| CSCsb23106 | Access | 7206vxr with NPE-G1 bus error crash when OIR PA-2T3+ |
| CSCsb27358 | Access | PA-T3+ goes down when seeing two bursts of AIS less than 1 second each |
| CSCsb29894 | Access | Frame relay input errors and CRC errors with reload and rpr+ switchover |
| CSCsb83876 | Access | Interface counters stop incrementing on serial interface counter |
| CSCsc48543 | Access | shot down E3 controller via SNMP crash the c7200 device |
| CSCsc66658 | Access | Interfaces starts toggling when loopback local configured |
| CSCsc85029 | Access | AIS led on pa-mc-2t3+ remains on if t3 connected after reload |
| CSCsc91995 | Access | Spurious memory access T3 Flexwan |
| CSCsd41989 | Access | ct3 pa: t3 controller stays down for local loopback in flexwan |
| CSCse06752 | Access | LAM /32 cef entry shows unresolved |
| CSCdy11156 | ATM | 13E:12E:RP crashed while applying config on ATM-PA,mgd_timer_stop . |
| CSCea26450 | ATM | PVC may stay down when interface cable is pulled out/put back rapidly |
| CSCef62324 | ATM | router may crash upon removal of ATM subinterface with PVCs |
| CSCeg03837 | ATM | ALIGN-3-SPURIOUS traceback in Standby RP when subinterface is configured |
| CSCeh71960 | ATM | alignment traceback on standby RP |
| CSCei39688 | ATM | ATM subinterface fails to pass traffic due to CEF initialization failure |
| CSCei45749 | ATM | PVCs go inactive when clear interface atm3/ima0 command is issued |
| CSCek39364 | ATM | CLI: HA Standby router reloads while unconfiguring atm bundle . |
| CSCek39946 | ATM | Local Switching connectivity not recovering after switchover |
| CSCin94072 | ATM | Bundle master should have length zero and adj complete |
| CSCin95455 | ATM | Duplicate options displayed in connect command output . |
| CSCsa85850 | ATM | PA-A3 allows to configure CBR at 155000 kbps . |
| CSCsb12329 | ATM | ifAdminStatus of ATM sub-interface is down without shutdown command |
| CSCsc49134 | ATM | Router crashes while creating ATM subinterface - ATM pvc discovery |
| CSCsd73881 | ATM | Router gets reloaded at process_ok_to_reschedule . |
| CSCsd88636 | ATM | Continuous RP CPUHOG by ATM OAM Input process |
| CSCsh39541 | ATM | CEF adjacency shows incomplete on ATM int with SUP4 . |
| CSCsh74025 | ATM | clns packets not being punted by an enhanced flexwan . |
| CSCdx54940 | Cisco IOS | CPU utilization in 3660 is 98% with aal2 calls |
| CSCea16744 | Cisco IOS | GBIC optical 7500 router crash on attach queueing output policy |

| Identifier | Technology | Description |
|---|---|---|
| CSCea24341 | Cisco IOS | SLB real to real ICMP traffic broken with FWLB |
| CSCeb77318 | Cisco IOS | IOS SLB: Incorrect checksum of forwarded icmp unreachable |
| CSCed15183 | Cisco IOS | Verify ATA is supported but msg says it is not |
| CSCed26241 | Cisco IOS | BootP Requests Modified in 12.2(15)BC1 |
| CSCed94829 | Cisco IOS | IOS reloads due to malformed IKE messages |
| CSCee66208 | Cisco IOS | Not able to remove port config using no port under DFP |
| CSCee79634 | Cisco IOS | Avert: IP phone is not statically authenticated on 831 using CDP |
| CSCee84918 | Cisco IOS | DHCP snooping on 3550 drops DHCPNAKs recieved when renewing old IP |
| CSCef82820 | Cisco IOS | Loadbalancing with >= 3 links in AToM cause VC to be down or crash |
| CSCeg02918 | Cisco IOS | Bus Error at auth_proxy_proc_profile |
| CSCeg41161 | Cisco IOS | Implementation of RM aging feature for EARL7 systems |
| CSCeg76039 | Cisco IOS | Show archive log config: conf terminal, exit, ctrl+z logged |
| CSCeh06200 | Cisco IOS | No HTTP access via TACACS if idle time configured on TACACS server |
| CSCeh12640 | Cisco IOS | show diag # performs show diagbus # instead of amb. command msg |
| CSCeh21210 | Cisco IOS | MF: DHCP Snooping crash when server send invalid option 82 |
| CSCeh35237 | Cisco IOS | 7600: 6748GE LC OIR causes spurious mem access and traceback |
| CSCeh42348 | Cisco IOS | PP:CWAN-QOS:DWRED is broken |
| CSCeh42472 | Cisco IOS | Standby RSP doesnt boot because of image uncompression failures |
| CSCeh51550 | Cisco IOS | SCP Health:LCs not responding to SCP keepaliaves after rpr+ for long |
| CSCeh56402 | Cisco IOS | Shutting peer FR link crashes router |
| CSCeh63002 | Cisco IOS | id_alloc_util_free should check for already freed ids |
| CSCeh78028 | Cisco IOS | 7600 Port-Sec: traffic fails to recover after reload |
| CSCeh78345 | Cisco IOS | Ensure EEM policies close tty session properly upon exit. |
| CSCei00856 | Cisco IOS | CWAN-QOS:oc-3:col2 crash with external memory address |
| CSCei08288 | Cisco IOS | show run misses no errdisable detect cause udld command |
| CSCei09247 | Cisco IOS | Local serial link goes up/down when remote link is admin down |
| CSCei27448 | Cisco IOS | Router crashes while displaying sh ip pim mdt bgp |
| CSCei37672 | Cisco IOS | chevys/c2lc take ~ 180s before resetting following a mandatory proc exit |
| CSCei38036 | Cisco IOS | layer 2 entry not removed when no int vlan |
| CSCei41088 | Cisco IOS | MVPN Tunnel interface not created with BGP Confedetration |
| CSCei46182 | Cisco IOS | c6msfc2a/sup32 DEC MOP packet internally looping |
| CSCei48635 | Cisco IOS | ChOC3/STM-1 SPA: many MFR interfaces remain down following microcode |
| CSCei51175 | Cisco IOS | PP:R3:SIP-200:1490 bridging - CPU1 crash with egress pol on main int |
| CSCei52830 | Cisco IOS | Banner command sync is broken by CSCin86483 . |
| CSCei55605 | Cisco IOS | Getting Traceback on the router while scheduling Kron |
| CSCei58681 | Cisco IOS | port channel does not form after minlinks added and removed |
| CSCei59601 | Cisco IOS | router crashes at ac_switching_validate_fibidb |

| Identifier | Technology | Description |
|---|---|---|
| CSCei68902 | Cisco IOS | Maverick: MFR interfaces could be down after SPA/router reload |
| CSCei72033 | Cisco IOS | 1xcSTM-1 SPA goes OOS upon adding 12 serial links to MFR bundle |
| CSCei73829 | Cisco IOS | Phase 2 Rekeying with VPN Client results in volume lifetime of 0 |
| CSCei74749 | Cisco IOS | port is suspended on the standby due to flowcontrol parameters |
| CSCei79969 | Cisco IOS | Traceback at issu_rcv_transform found on PE after VPN SSO |
| CSCei80699 | Cisco IOS | multicast tunnel if_number numbers being duplicated |
| CSCei86192 | Cisco IOS | PP:R3:FlexWAN+PA-8xT1/E1: RP crashed MALLOCFAIL due to loveletter |
| CSCei86256 | Cisco IOS | Crash when typing show lacp neighbors |
| CSCei86313 | Cisco IOS | PP:R3:FW+8xT1/E1:Stuck in LOS state after card type E1 provisioned |
| CSCei90238 | Cisco IOS | Rainier:SIP-200: %C7600_SIP200_MP-4-PAUSE @tal_tree_item_delete |
| CSCei92291 | Cisco IOS | Message on reload:Error in setting Reload Reason |
| CSCei93025 | Cisco IOS | Etherchannel config changes not synched to inactive member ports |
| CSCei95384 | Cisco IOS | PP:R3:8xT1/E1-SPA MLP: EFC ERROR/inactive after link added to bundle |
| CSCej02181 | Cisco IOS | SLB: cannot configure weight 0 |
| CSCej08637 | Cisco IOS | Inline power sensors needed on standby to support entity mib SSO. |
| CSCej13660 | Cisco IOS | mem leak from MallocLite allocated by crypto_kmi_add_data_to_pyld |
| CSCej16004 | Cisco IOS | ML MTU cfg from CLI does not change the MTU operation |
| CSCej21515 | Cisco IOS | ATM SPA DLL tuning may miss valid lock points |
| CSCej21520 | Cisco IOS | ATM SPA: Removing APS on Protect interface causes locked console |
| CSCej27397 | Cisco IOS | CT3 SPA: add firmware support to allow host to set overflow threshol |
| CSCej37803 | Cisco IOS | cT3 SPA:Upgrade to IOFPGA rev2.1 |
| CSCej63166 | Cisco IOS | %LSD-4-LABEL_RESOURCE: label range is not freed |
| CSCej70453 | Cisco IOS | Unable to control application: OER Route Map Failure |
| CSCej83531 | Cisco IOS | isakmp sa is not up in change_hostname_ip |
| CSCej86188 | Cisco IOS | MLS packet error syslogs should be configurable and no service int |
| CSCek03772 | Cisco IOS | zamboni: crashes for double fragmentaion |
| CSCek22536 | Cisco IOS | SLB high cpu with second VIP inservice and user->real traffic |
| CSCek22595 | Cisco IOS | SLB vserver access commands break user->real traffic |
| CSCek22782 | Cisco IOS | CSM: Configuration sync check does not work in all cases |
| CSCek24053 | Cisco IOS | Sup720_rp: spurious memory accesses in cardifmib_get_card_index |
| CSCek25660 | Cisco IOS | tarceback found at l2_modify_one_entry(0x207b9614)+0x48 . |
| CSCek26158 | Cisco IOS | IOS TCL leaks memory when EEM policy triggered. |
| CSCek26296 | Cisco IOS | PR+:p-map with a single band+shape class doesnot guarantee bandwidth . |
| CSCek26742 | Cisco IOS | Rainier:SPA-8XCHT1/E1: All T1/E1s in DOWN after RPR+ switchover |
| CSCek28110 | Cisco IOS | TB @ xdr_lc_check_sequence %XDR-SP-3-XDROOS rcvd after multilple SSO |
| CSCek28561 | Cisco IOS | SIP1/ChOC3: T1/E1 BERT unusable after first run |
| CSCek30152 | Cisco IOS | Error in calculation subrate bandwidth for Kentrox mode . |

| Identifier | Technology | Description |
|---|---|---|
| CSCek31059 | Cisco IOS | mvpn:duplicate pkts are seen while crossing multiple PEs |
| CSCek31610 | Cisco IOS | IOS changes to support sticky replication in CSM |
| CSCek31960 | Cisco IOS | ping failed when core configured with GRE tunnel |
| CSCek32555 | Cisco IOS | MFR i/f lineprotocol takes too long to come up after RPR+ switch |
| CSCek35321 | Cisco IOS | ifStackTable has 2 lower layers for 4chstm1 e1 ds1 layer |
| CSCek35767 | Cisco IOS | Need show mls statistics protocol equivalent in IOS |
| CSCek35770 | Cisco IOS | Need show module power equivalent in IOS |
| CSCek35773 | Cisco IOS | Need show mls multicast router equivalent options in IOS |
| CSCek35951 | Cisco IOS | Priority queue with policing configured doesnt work |
| CSCek36014 | Cisco IOS | Need show version epld equivalent in IOS |
| CSCek37181 | Cisco IOS | Loopback on controller for online diagn of wism card |
| CSCek37494 | Cisco IOS | mls acl tcam share-global should not be NVGENed |
| CSCek37963 | Cisco IOS | 1st level WRED faild with Policer in 1st & 2nd level . |
| CSCek39186 | Cisco IOS | MAC-address for HSRPs VIP not in FVRF vlan if tunnel redirected . |
| CSCek39392 | Cisco IOS | Crash @ registry_add_list when loading IOU/unix-p-ms image |
| CSCek42027 | Cisco IOS | SPA FPD upgrade fails with sip1-CR |
| CSCek43497 | Cisco IOS | IBM/JDSU type SFP not work with latest rainier image |
| CSCek44502 | Cisco IOS | 6vpe:QoS classify counter not working . |
| CSCek45036 | Cisco IOS | Interuppt throttling to be implemented for Sibyte Modular IOS images. |
| CSCek45862 | Cisco IOS | set mpls exp impositon not working with 6PE IPv6 traffic on SIP-200 |
| CSCek47083 | Cisco IOS | B2B:ad erros on active blade when both blades are reloaded . |
| CSCek47205 | Cisco IOS | B2B:PKI:Crash at bitlist_validbit |
| CSCek47574 | Cisco IOS | SIP 400 drop mpls packets and cause traceroute fails |
| CSCek48252 | Cisco IOS | RRI current peer not set specifically in case of QM retrans fail |
| CSCek50172 | Cisco IOS | %SYS-3-TIMERNEG: Cannot start timer with negative set |
| CSCek50720 | Cisco IOS | Improve error handling for DLL centering algorithm |
| CSCek53756 | Cisco IOS | %SYS-3-INTPRINT: Illegal printing attempt from interrupt level on LC |
| CSCek54572 | Cisco IOS | crash at ace_create_cm_head_node . |
| CSCek54959 | Cisco IOS | %MFI-3-REDISTMGR %LFD-3-BADEXEC %LFD-3-SM upon SSO Switchover |
| CSCek55639 | Cisco IOS | Failed to assert Physical Port Administrative State Down alarm |
| CSCek55870 | Cisco IOS | fabric buffer-reserve queue default issues |
| CSCek57760 | Cisco IOS | IP MTU of GRE tunnel not used by SPA-IPSEC |
| CSCek58678 | Cisco IOS | %SYS-3-INTPRINT: Illegal printing attempt from interrupt level on LC |
| CSCek60775 | Cisco IOS | Router crashed at ace_clear_local_address after change to VIP addres . |
| CSCek61974 | Cisco IOS | Minimum configurable rx timers should be greater than 1 |
| CSCek63611 | Cisco IOS | rekey fails after crypto card is rebooted . |
| CSCek65022 | Cisco IOS | 7600-SSC-400: SPA-IPSEC-2g EFC clock hardware issue . |

| Identifier | Technology | Description |
|---|---|---|
| CSCek65087 | Cisco IOS | Traceback see at unqueue while running cef_tunnel_vrf script |
| CSCek66277 | Cisco IOS | Diagnostics test 18 TestAclDeny should be marked Disruptive . |
| CSCek66294 | Cisco IOS | TCP adjust mss on egress direction |
| CSCek66590 | Cisco IOS | C7600-SSC-400: Crash in show hw-m subslot x status volt |
| CSCek66842 | Cisco IOS | 12.2SRB: OER netflow enabling broken . |
| CSCek66877 | Cisco IOS | %XDR_SP-STDBY-6-CLIENTISSU_BLOCKED: XDR client lte broker cannotSync |
| CSCek67100 | Cisco IOS | Cheronia: Crashinfo write fails |
| CSCek67622 | Cisco IOS | BFD should not be configurable on etherchannel intf |
| CSCek67701 | Cisco IOS | SPA-IPSEC-2G: Crashdump not getting saved on NMI . |
| CSCek68108 | Cisco IOS | Router crashed at ace_policyloader_util.c after remove crypto map . |
| CSCek68218 | Cisco IOS | sip-600 crashing with diagnostics error online_wan_diag_rp_request |
| CSCek68265 | Cisco IOS | Major alarm on active caused syst. shutdn instead of swover to stdby |
| CSCek68281 | Cisco IOS | Syslog instead of crashing on correctable FIB SSRAM ECC errors |
| CSCek68800 | Cisco IOS | mls error action freeze default to change from freeze to reset |
| CSCek68890 | Cisco IOS | After reload 2 Zamboni, routing adj not come up over some tunnels . |
| CSCek70014 | Cisco IOS | Need a way to clear diagnostic event log |
| CSCek72777 | Cisco IOS | %CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR for 7600 SIP card . |
| CSCek73332 | Cisco IOS | Bidir shadow entry is missing some interfaces in oif |
| CSCek74858 | Cisco IOS | glbp weighting track config sync failure |
| CSCek75768 | Cisco IOS | Ensure EEM policies are registered correctly through ssh. |
| CSCek78219 | Cisco IOS | SIERRA: Active Sierra Stnby Boomerang -- stdby crashes in IPC on bootup |
| CSCin78110 | Cisco IOS | Some E1 controller does not come up if a large config on other LC |
| CSCin89551 | Cisco IOS | VIP crash at dmfr_fastsend when pumping traffic via dMFR bundles. |
| CSCin97815 | Cisco IOS | FRF.16 - blt counters not updated to RP after reload of router |
| CSCin97912 | Cisco IOS | FESPA-SIP1:After LC reset, Intf comes as up-up even if peer is down |
| CSCin98448 | Cisco IOS | controller shut throws up error msg and remote end is not going down |
| CSCir01217 | Cisco IOS | name_svr.proc[64]: Could not register interest |
| CSCsa54688 | Cisco IOS | %IDBINDEX_SYNC-3-UNKNOWN_TYPE: IDB type is unknown after switchover |
| CSCsa56229 | Cisco IOS | Traceback mesg seen when standby SUP comes online on Port security |
| CSCsa57524 | Cisco IOS | Incorrect SPA GE-WAN main interface IF-MIB Counter Support |
| CSCsa58703 | Cisco IOS | Not all ATM ACs indicated up via show mpls l2tr sum using PW redundancy |
| CSCsa61687 | Cisco IOS | c12000 crashes by issuing show sss cmd. |
| CSCsa66683 | Cisco IOS | Enhance bridged flow stats to support l2 vlans |
| CSCsa71295 | Cisco IOS | show mod indicates Unknown diag status for SIP cards after switchover |
| CSCsa75094 | Cisco IOS | po based eompls pkst not hitting eom adj until po shut/unshut |
| CSCsa76016 | Cisco IOS | NAT netflow entyr created without reason |
| CSCsa76801 | Cisco IOS | Major bootup failure on Sup720 causing other linecards to PwrDown |

| Identifier | Technology | Description |
|---|---|---|
| CSCsa77785 | Cisco IOS | Router crashes when L2 redirection is configured with HTTP traffic |
| CSCsa79561 | Cisco IOS | Any type 6 key with arbit length crashes the router |
| CSCsa79630 | Cisco IOS | Cat6500 Netflow does not export all flows |
| CSCsa80358 | Cisco IOS | Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks |
| CSCsa80620 | Cisco IOS | ct3 spa: serial interface efc queue stuck on deleting/adding mlp bundle |
| CSCsa87316 | Cisco IOS | Issuing interface ATM/IMA may result in an unexpected reload. |
| CSCsa91478 | Cisco IOS | L2TPV3: SW_MGR-3-CM_ERROR:Connection Manager Error - unprovision segment |
| CSCsa94234 | Cisco IOS | GTP SLB : Sticky timer should be atleast greater than Session Timer |
| CSCsa95306 | Cisco IOS | SNMPWALK does not get all CSG user group information |
| CSCsa96960 | Cisco IOS | ip ttl expired lsp ping pkts shouldn'tt be transited by MFI process sw |
| CSCsa97042 | Cisco IOS | Secured port dropping traffic after applying & removing mac-filter |
| CSCsa99158 | Cisco IOS | Unexpected START records triggered by IPSec - unreliable AAA records |
| CSCsa99983 | Cisco IOS | FR VC is up but not passing traffic with L2TPv3 |
| CSCsb11224 | Cisco IOS | system crashes soon after changes in cos-mutation map |
| CSCsb12969 | Cisco IOS | MQC: Router crashes when a service-policy is added to atm or FR pvc |
| CSCsb13358 | Cisco IOS | failaction gtp purge doesnt delete some gtp stickies when probe fail |
| CSCsb14516 | Cisco IOS | SYS-3-INTPRINT errors seen when ACL used as route-map match criteria |
| CSCsb14543 | Cisco IOS | t/b  pm_port_counters_lock on module reset of active supervisor |
| CSCsb18498 | Cisco IOS | SNMP polling broken in cat6k SXE1 image |
| CSCsb26172 | Cisco IOS | Rollback: Timed Rollback option is not available. |
| CSCsb29028 | Cisco IOS | Processor Memory leak in Crypto IKMP process |
| CSCsb31368 | Cisco IOS | ATM Multipoint bridging on c65xx is broken after SW upgrade |
| CSCsb33258 | Cisco IOS | RP crash while mvpns come up - MDFS buildup |
| CSCsb36463 | Cisco IOS | RF-bit not set in the DBUS hdr for the FS switched+RTD port snooped pkt |
| CSCsb40858 | Cisco IOS | IP packets with ip options sourced from TE head fails for 1 hop tunnels. |
| CSCsb41923 | Cisco IOS | isakmp key ending in backslash  will be lost after device reboot |
| CSCsb42176 | Cisco IOS | PA-POS-2OC3: router hang upon neighbor reload |
| CSCsb48739 | Cisco IOS | GTP SLB:Session reassigned even when sticky entry exists |
| CSCsb53810 | Cisco IOS | sup720 outbound acl not denying traffic, hitting incorrect tcam entry |
| CSCsb54233 | Cisco IOS | ISIS hello not rcved on  dot1q sub interface on a  WS-X6582-2PA |
| CSCsb56931 | Cisco IOS | The SWIDB subblock named QM was not removed, on PPP to FR encap change |
| CSCsb57042 | Cisco IOS | %SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs |
| CSCsb59349 | Cisco IOS | Standby RP crashed on applying policy to 1k SVI |
| CSCsb60453 | Cisco IOS | Need improved logs for severe fabric errors which triggers fab swover |
| CSCsb61021 | Cisco IOS | IP Spoofed packets from CE are not hw switched with egress WCCP |
| CSCsb62773 | Cisco IOS | Guaranteed bandwidth not consistent with hier shaping configured |
| CSCsb63267 | Cisco IOS | Error locating default vpn |

| Identifier | Technology | Description |
|---|---|---|
| CSCsb65595 | Cisco IOS | TCAM LOU expansion doesnt work properly for IPv6 . |
| CSCsb67152 | Cisco IOS | MET inconsistent on DFC, multicast traffic is blackholed for an OIF |
| CSCsb68178 | Cisco IOS | Traceback Seen @ %MPLS_IPRM-3-DB_PATH on 6VPE |
| CSCsb68513 | Cisco IOS | Mcast packets not always forwarded through VPNSM on 6500 with SUP720 |
| CSCsb70335 | Cisco IOS | Flexwan crash when fragmentation is enabled under MFR interface |
| CSCsb70973 | Cisco IOS | igmp snooping explicit tracking and report suppression issues |
| CSCsb70996 | Cisco IOS | IOS SLB drops trailing fragments in VRF and misroutes SLB msgs to GGSN |
| CSCsb71242 | Cisco IOS | MMLS NSF/SSO: Mcast Failover time very high for the first switchover |
| CSCsb74212 | Cisco IOS | Logical & Phy Port run Configs lost on toggling no sw / sw frm VTY |
| CSCsb76401 | Cisco IOS | config mode locks out when u boot active and standby with differ images |
| CSCsb77716 | Cisco IOS | dot1x:SP crash at sm_destroy_instance on OIR or link flap |
| CSCsb80141 | Cisco IOS | IOS-SLB: no mls ip slb search icmp does not work. |
| CSCsb80590 | Cisco IOS | Enhance IPC buffer usage and IOMEM buffer allocation for Flexwan |
| CSCsb84998 | Cisco IOS | MLS-MSC ASSERTION FAILED with T/Bs after hw-module reset |
| CSCsb85030 | Cisco IOS | lost connectivity after port security disabled/removed - packets drop |
| CSCsb85049 | Cisco IOS | cwpa2 bridged/routed ATM PDUs lost between Flexwan2 and SUP720 |
| CSCsb85927 | Cisco IOS | Routes not deleted on the EzVPN Vi server |
| CSCsb86198 | Cisco IOS | show port-sec int <int-name> add not sync with stdby after SO |
| CSCsb89241 | Cisco IOS | BRE LTL is not populated properly after reload for flexwan2 |
| CSCsb89847 | Cisco IOS | Source and destination BGP AS not being exported correctly with Netflow |
| CSCsb89891 | Cisco IOS | dhcp snooping traceback on sup720 |
| CSCsb91644 | Cisco IOS | IPv6 MFIB entry is updated on RP and delayed to update MFIB on SP & DFC |
| CSCsb94412 | Cisco IOS | SIP1: RBE: OAM Packets being accounted as input errors |
| CSCsb94859 | Cisco IOS | ATOM_TRANS-3-CONSISTENCY observed Pseudowire Reundancy |
| CSCsb95563 | Cisco IOS | cat6k crashes while releasing mem blocks after unconfig regd. EM Policy |
| CSCsb95851 | Cisco IOS | Cat6K crashing by bus error at msc_sc2vdb_unlink |
| CSCsb98702 | Cisco IOS | Breakpoint (signal 5 exception) when ltl profiling . |
| CSCsc01223 | Cisco IOS | E5 L2TPv3 SCALE: Not all sessions are coming up on router reload |
| CSCsc02537 | Cisco IOS | Add error message when sh frame-relay frag executed for hw mfr/frf.1 |
| CSCsc04015 | Cisco IOS | cbQosCMStatsTable doesn't return byte statistic for FastEthernet PAs |
| CSCsc05500 | Cisco IOS | ENTITY-MIB: SFP in Gi1/1 is not displayed in show inventory |
| CSCsc08498 | Cisco IOS | SCHED-3-THRASHING traceback from MWAM_CONSOLE Background Process |
| CSCsc08602 | Cisco IOS | RLB errors with code 50 and access messages without username |
| CSCsc08947 | Cisco IOS | 6k IOS Autostate: L3 int up/up if last L2 port disabled while L3 is shut |
| CSCsc09557 | Cisco IOS | Dot1x authenticated ports loosing states after SSO |
| CSCsc13720 | Cisco IOS | llq functionality with _match input vlan_ broken |
| CSCsc16508 | Cisco IOS | dmfr: VIP may crash @mfr_print on enabling debug dmfr packets |

| Identifier | Technology | Description |
|---|---|---|
| CSCsc18551 | Cisco IOS | Spurious Access on OSM line card |
| CSCsc18728 | Cisco IOS | Sup720 HW PAT (NAT overload) punts frames with valid MTU |
| CSCsc18986 | Cisco IOS | IOS SLB causes high CPU |
| CSCsc21417 | Cisco IOS | OER does not work with NAT |
| CSCsc21446 | Cisco IOS | Multiple IKE SAs created |
| CSCsc24102 | Cisco IOS | Fabric sync errors if WS-X6704-10GE is on slot 4 on 7606 |
| CSCsc25952 | Cisco IOS | Need to print out error message for unsupported marking on OSM |
| CSCsc26048 | Cisco IOS | Cat6k: CPUHOG in PIM Snooping Process |
| CSCsc26490 | Cisco IOS | wrong static mac address entry in case of GLBP virtual mac |
| CSCsc28781 | Cisco IOS | %PM-SP-STDBY-3-INTERNALERROR: Port Manager Internal Software Error (pd ! |
| CSCsc29022 | Cisco IOS | c7500 -- Broken policy on MFR causing wrong SNMP counters |
| CSCsc29320 | Cisco IOS | Ezvpn server doesn't show number of connections in show crypto session |
| CSCsc30268 | Cisco IOS | linecards crash @ free_qos_set_if_sub_structures |
| CSCsc30532 | Cisco IOS | PIM snooping not populating mac-address table properly on auto rp group |
| CSCsc32189 | Cisco IOS | ISAKMP does not check multiple transform payloads in one proposal . |
| CSCsc32248 | Cisco IOS | Multiple IKE SAs if packets destined to unreachable addresses |
| CSCsc32801 | Cisco IOS | Traceback seen after configuring 8 channel-members in etherchannel |
| CSCsc33110 | Cisco IOS | Sip-400 MPB: ST instance not created on SUPW when a PVC is created |
| CSCsc37514 | Cisco IOS | Pseudowire: LSP ping output |
| CSCsc43862 | Cisco IOS | SPA ping failure caused by SIP-200 serial primary channel sync failure |
| CSCsc46301 | Cisco IOS | Crash in GTP SLB imsi sticky |
| CSCsc46922 | Cisco IOS | Memory leak - SSM segments |
| CSCsc48715 | Cisco IOS | LFIB does not install  both adjacency with Load balancing |
| CSCsc48986 | Cisco IOS | WS-X6148-FE-SFP boards may fail to bootup in Supervisor IOS |
| CSCsc52306 | Cisco IOS | IDSM: span tree not blocking when two IDSM in inline mode |
| CSCsc52645 | Cisco IOS | SIP1-CT3: Whole T1 goes down while doing timeslot BERT on CT3 SPA |
| CSCsc54584 | Cisco IOS | Ingress standard ACL for transit traffic broken with MFR bundle |
| CSCsc55229 | Cisco IOS | FWSM rebooting continously |
| CSCsc55949 | Cisco IOS | C2 Frequent fabric channel sync errors and rxErrors |
| CSCsc55951 | Cisco IOS | SPA-4XOC3-ATM has compatibility issue with 3rd vendor device |
| CSCsc56179 | Cisco IOS | mac-address is not purge when interface is shutdown . |
| CSCsc57156 | Cisco IOS | Hardware fault on FWSM ports not causing FWSM redundancy failover |
| CSCsc58025 | Cisco IOS | Out of Service |
| CSCsc59025 | Cisco IOS | UDLD config on 2nd uplinki of act/sby sup change after switchover |
| CSCsc59190 | Cisco IOS | %PM-STDBY-4-INT_FAILUP: fa4/3 failed to come up message after switchover |
| CSCsc61086 | Cisco IOS | TCAM entry optimization needed for NAT outside i/fs with big NAT cfg |
| CSCsc61257 | Cisco IOS | Software watchdog timeout in Active-SP causes both sups to crash/reload. |

| Identifier | Technology | Description |
|---|---|---|
| CSCsc61809 | Cisco IOS | Min-links feature doesn't work intermittently even just on shut/no shut |
| CSCsc61899 | Cisco IOS | SIP1-ChOC3: HDLC Controller Device driver Failure (linkrec error) |
| CSCsc64718 | Cisco IOS | persistent-store command not available on SUP32 Images |
| CSCsc65256 | Cisco IOS | Connection Count incorrect after ungraceful disconnect/reconnect |
| CSCsc65787 | Cisco IOS | Enhance (or remove) the automatic intf MTU changing logic in CSCsa73817 |
| CSCsc68250 | Cisco IOS | Packet flow halt on 7600-SIP-400 |
| CSCsc68615 | Cisco IOS | Router Crash %CPU_MONITOR-3-PEER_EXCEPTION IPv6 IP Tunnel |
| CSCsc69076 | Cisco IOS | SIP1-ChOC3: Spurious access at swsb_delete on unconfig of T1 chnl group |
| CSCsc69851 | Cisco IOS | Port Security does not show offending MAC address in syslog |
| CSCsc71051 | Cisco IOS | VIP4-80 crashed with multilink frame relay configure and L2TPv3 |
| CSCsc71245 | Cisco IOS | sup720:High CPU and traceback in ipsec_db_get_ipsec_sa_list with VPNSM |
| CSCsc75397 | Cisco IOS | sup32 enables fix for CSCeb49514 with cross-module etherchannel |
| CSCsc77287 | Cisco IOS | SIERRA: Telnet/console: freeze by remote command module slot |
| CSCsc77455 | Cisco IOS | Fabric counters are inconsistent |
| CSCsc78707 | Cisco IOS | xconnect: l2transport option not valid on dot1q interfaces |
| CSCsc80303 | Cisco IOS | %IPC-SP-5-WATERMARK: 7167 messages pending in rcv for the port Card7/0: |
| CSCsc80822 | Cisco IOS | VPN-SPA - Router fails to decrypt certificate payload during IKE negotia |
| CSCsc81495 | Cisco IOS | PWAN2 HQoS packets dropped with on-the-fly policymap modification |
| CSCsc81834 | Cisco IOS | Netflow uses incorrect source ip address if its within MPLS vrf |
| CSCsc83961 | Cisco IOS | Both APS protect & working ports forwarding traffic |
| CSCsc84768 | Cisco IOS | FESPA-SIP1:BFD session parameter configuration lost on SPA s/w OIR |
| CSCsc86600 | Cisco IOS | SNMP:subinterface aal5 layer: Ifindex counter for ATM SPA not updated |
| CSCsc89044 | Cisco IOS | IO memory leak with big buffers and EOBC0/0 |
| CSCsc89229 | Cisco IOS | Traceback  & crash at pm_get_standby_vlan on Sup720 |
| CSCsc89932 | Cisco IOS | Switch crash after running show diagnostic sanity command |
| CSCsc89979 | Cisco IOS | EEM traceback for,action x info cli frequenc; if cli history table empty |
| CSCsc90782 | Cisco IOS | dsx1FarEndInterval not available in 12.2(18)SXF on a c7609 |
| CSCsc91075 | Cisco IOS | IPSEC Connection Count incorrect after unsuccesfull connection attempt |
| CSCsc93283 | Cisco IOS | R2.5: no mls qos mpls trust exp CLI not effective after reload |
| CSCsc94402 | Cisco IOS | DHCP snooping error msg dispalyed continuously on console |
| CSCsc96158 | Cisco IOS | VPNSM / VPNSPA: IKE SA not deleted even after IPSEC SA idles out. |
| CSCsc98850 | Cisco IOS | ZAMBONI:Could not send pmtu information vlan 65535 pmtu 0 Error |
| CSCsd00258 | Cisco IOS | ENH - Syslog msg - exceeding broadcast suppression threshold |
| CSCsd00694 | Cisco IOS | Need to use L2 port mac for pagp bpdu's to work with cat5000 |
| CSCsd01719 | Cisco IOS | SIP-600: SPA OIR with DOT1Q tunnel on port-channel can crash RP |
| CSCsd01885 | Cisco IOS | Flexwan module, when pvc is down, mac-address are not flushed |
| CSCsd03220 | Cisco IOS | OER NFC: stats for default route not aggregated. |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd03416 | Cisco IOS | Active RP Crashed after doing rerouting in PIM SM Stress Test |
| CSCsd03960 | Cisco IOS | OSM shaping parameter not programmed correct |
| CSCsd04808 | Cisco IOS | ROOT_Inc message is not show up for all mst instance |
| CSCsd05513 | Cisco IOS | 7600 CBQOS-MIB is missing info which is present in CLI |
| CSCsd08411 | Cisco IOS | EEM Tcl policy execution delayed relative to config size |
| CSCsd09324 | Cisco IOS | IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP shown on stby RP when reload rtr |
| CSCsd13448 | Cisco IOS | IOS SLB custom udp probes don't support faildetect |
| CSCsd15625 | Cisco IOS | CEF Adjacencies not established with sub-interfaces configured |
| CSCsd17174 | Cisco IOS | SLB Connection states get  into loop on snmp query |
| CSCsd17992 | Cisco IOS | After PS fails and powered on, PS fan fail msg. display even if PS on |
| CSCsd18278 | Cisco IOS | Host backpressure is not handled by SPA IPC firmware code |
| CSCsd18296 | Cisco IOS | Bdwth guarantee not met in  cbwfq when cfged with llq in child in MIV . |
| CSCsd19181 | Cisco IOS | Crypto connect command is dropped from serial interface after reload . |
| CSCsd19203 | Cisco IOS | SIP400:ATM:new LLQ traffic stop flowing on dynamic changes to Policy |
| CSCsd22834 | Cisco IOS | SIP1-ChOC3: Tx CPU suspended for too long @tal_tree_item_insert |
| CSCsd23454 | Cisco IOS | NPE-G2 VAM2+ : Mem increase at crypto_ipsec_sa_lookup_insert key eng |
| CSCsd25532 | Cisco IOS | High SP-CPU utili occurs when c7600 recieves IPv6 Multicast traffic |
| CSCsd25611 | Cisco IOS | MPLS VPN forwarding broken for new vrfs on PE 7600 SUP720 |
| CSCsd25653 | Cisco IOS | vrf-also in named ACL for VTY line not saved in running configuration |
| CSCsd28910 | Cisco IOS | Port put in err-disable due to link flaps while other end reloads |
| CSCsd29911 | Cisco IOS | IPSLA : Issues with tracking command threshold weight up xx down xx |
| CSCsd29927 | Cisco IOS | 6500 BIT-SP-4-OUTOFRANGE error with voice vlan dot1p and monitor session |
| CSCsd30533 | Cisco IOS | Duplicate ipsec flows at the hub created when spoke is behind nat device |
| CSCsd32192 | Cisco IOS | GRE Tunnel With Checksum Enabled Does Not Transmit Multicast Packets |
| CSCsd32634 | Cisco IOS | R3.2:IOS:Sup32 crashed after range of vlans 1-4094 has been configured . |
| CSCsd33992 | Cisco IOS | %PM-SP-STDBY-3-INTERNALERROR: when boot up |
| CSCsd35622 | Cisco IOS | session timeout TCL causes CPU hog/crash |
| CSCsd36670 | Cisco IOS | Can not enable cdp globally from SNMP |
| CSCsd38305 | Cisco IOS | crash Ethchnl assert (group>=1)switch_private.c:38 after EC remote chang |
| CSCsd40211 | Cisco IOS | Sup720 : Delay in arp result after interface shut/no shut |
| CSCsd42319 | Cisco IOS | SIP400 crashes during bootup with current pikespeak image |
| CSCsd43481 | Cisco IOS | EoMPLS drops OSPF multicast packets with mls ip verify length minimum |
| CSCsd45167 | Cisco IOS | Memory leak in Crypto IKMP Process |
| CSCsd45932 | Cisco IOS | Rainier: On an idle SIP-200 with any chann SPA, CPU util is 10% per SPA |
| CSCsd46882 | Cisco IOS | OSM-CT3  Port in Unchannelized mode stays UP/UP when looped towards line |
| CSCsd47475 | Cisco IOS | cat6k unable to resolve arp request when using flexwan, pa-fe-tx and vpn |
| CSCsd47734 | Cisco IOS | Additional memory leak fixes by ActiveState |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd48741 | Cisco IOS | DFC does not see sampled netflow vlans after reload |
| CSCsd49280 | Cisco IOS | show idprom should work with non-cisco xenpaks |
| CSCsd49374 | Cisco IOS | CT3 SPA:%SPA_CHOC_DSX-3-SPA_CMD_SEND_ERR:, all intf stay down |
| CSCsd49862 | Cisco IOS | BFD session stays down after doing shu/unshut on vlan-bundle interface |
| CSCsd50828 | Cisco IOS | AS-path based redistribution fails |
| CSCsd51577 | Cisco IOS | bfd echo to no echo switch removes bfd monitoring |
| CSCsd52633 | Cisco IOS | VPN-Spa stop forwarding traffic if any changes on ATM traffic shaping |
| CSCsd53513 | Cisco IOS | %ALIGN-3-SPURIOUS_SO: Spurious memory access seen with tracebacks |
| CSCsd56549 | Cisco IOS | GRE doesnt get the same port that it req, PPTP change Call ID wrongly |
| CSCsd58181 | Cisco IOS | VIP4-80 Crash with ch-STM1 PA |
| CSCsd58422 | Cisco IOS | %IXP_MAP-3-QOS_CONFIG:  error detected: Can't download policymap |
| CSCsd58552 | Cisco IOS | cwpa2: TCP to NAT addresses cause FR encap change from IETF to cisco |
| CSCsd59274 | Cisco IOS | MLD snooping report-suppression does not work correctly |
| CSCsd59975 | Cisco IOS | WS-X6704-10GE causing CRC errors on WS-X6502-10GE interfaces |
| CSCsd63951 | Cisco IOS | sup720 ION: active crashes when slot 2 is reset |
| CSCsd64103 | Cisco IOS | 'mls qos trust dscp' not working for traffic coming from FWSM |
| CSCsd64224 | Cisco IOS | Memory leak in Crypto IKMP process when using certificate authentication |
| CSCsd64533 | Cisco IOS | Memory leak in Crypto IKMP process when using certificate authentication |
| CSCsd64640 | Cisco IOS | Memory leak in IPSEC key engine process with isakmp profiles |
| CSCsd64741 | Cisco IOS | SLB IMSI sticky idle timeout queries fail to reach GGSN when vrf-aware |
| CSCsd65434 | Cisco IOS | igmp snooping fails when leave is processed during igmp general query |
| CSCsd66276 | Cisco IOS | IDSM: monitor session dest config removed after two sso switchovers . |
| CSCsd66406 | Cisco IOS | SP error msg is not printed part of syslog levels |
| CSCsd67456 | Cisco IOS | VPN-SPA: IPSec SA comes up with wrong lifetime in KB |
| CSCsd68266 | Cisco IOS | input errors increment on 10/half port |
| CSCsd69480 | Cisco IOS | %HYPERION-4-HYP_RESET on flexwan2 chSTM1 card |
| CSCsd69842 | Cisco IOS | Memory leak in Crypto IKMP process on ezvpn server |
| CSCsd70321 | Cisco IOS | Resetting a line card and an sso right after that - traffic gets dropped |
| CSCsd70494 | Cisco IOS | Bidir-Multicast Packets are dropped when using G/m entries |
| CSCsd70948 | Cisco IOS | After SSO switchover all CDP and BPDU are lost if L2 rate limiting is on |
| CSCsd71047 | Cisco IOS | NAT cef entry is not changed after IP address change MAC address |
| CSCsd73598 | Cisco IOS | Rainier: TB points to mgd_timer_complain_uninit when remove bfd interval |
| CSCsd74729 | Cisco IOS | crypto map in vrf mode failed to create ipsec sa if fvrf != ivrf |
| CSCsd74975 | Cisco IOS | Clearly indicate customer friendly bus stall log messages. |
| CSCsd75069 | Cisco IOS | IPC RX FIFO FULL err w/ high traffic&LC CPU (IO-FPGA Pat-Mav2.5/Pro1.5) |
| CSCsd75836 | Cisco IOS | netflow removed from config at bootup due to CSCuk50395 |
| CSCsd75929 | Cisco IOS | Sup32 fails to get DHCP snooping binding table on switchover |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd77207 | Cisco IOS | Bidir traffic changed from HW to SW switch after add 200 sub-inf quickly |
| CSCsd78210 | Cisco IOS | FPD upgrade file search failed although the file is present. |
| CSCsd79536 | Cisco IOS | Standby RP crashes once at reload after installing set of patches . |
| CSCsd79558 | Cisco IOS | DMVPN:IPSEC SAs fail to get established with fvrf configured on tu |
| CSCsd80745 | Cisco IOS | bus error or alignment err at crypto_isakmp_profile_contain_xauth_info. |
| CSCsd80770 | Cisco IOS | Netflow exports UDP packets with source port 0 |
| CSCsd83402 | Cisco IOS | Large packets dropped when service policy applied |
| CSCsd84497 | Cisco IOS | auth-proxy requests stuck in init state |
| CSCsd86340 | Cisco IOS | After unplugging PC from back of phone into new port - error disable |
| CSCsd87313 | Cisco IOS | ip cef load-shar algorithm universal not consistent between stack member |
| CSCsd88586 | Cisco IOS | PBR : Wrong behaviour when first next-hop falls under a route to Null0 |
| CSCsd89949 | Cisco IOS | locIfReason is wrongly reporting admin down in an linkDown trap . |
| CSCsd90173 | Cisco IOS | TestIPSecEncrypDecrypPkt HM test config init error reporting is needed |
| CSCsd92208 | Cisco IOS | vlan map ocpu is wrong in the active vpnspa after sso+b2b failover . |
| CSCsd93294 | Cisco IOS | %SYS-STDBY-2-CHUNKFREE err and crash, points to chunk_free_with_pc |
| CSCsd94127 | Cisco IOS | COS aligned to IPP for routed multicast traffic |
| CSCsd94439 | Cisco IOS | I/O mem corruption on SP with mld snooping report-suppression enabled |
| CSCsd94541 | Cisco IOS | Multiple T3 controllers bounce on the SPA |
| CSCsd94936 | Cisco IOS | all interfaces are up/down after physical oir cable |
| CSCsd95575 | Cisco IOS | RP-Crash @ draco2_pa_eobc_intr |
| CSCsd95701 | Cisco IOS | CLI : sh mls qos ip <intf> shows intf disabled on vlan-based switchport |
| CSCsd95877 | Cisco IOS | %MLS_ACL_COMMON-SP-4-MLS_ACL_CONSIST appears on active SP on sso. |
| CSCsd96121 | Cisco IOS | Mac's don't get purged when the port is blocking during topology change |
| CSCsd96511 | Cisco IOS | Interface admin down: egress TCAM default program as bridge |
| CSCsd98390 | Cisco IOS | WS-X6148A-45AF module may not bootup/lose config on switch power-cycle. |
| CSCsd98852 | Cisco IOS | EEM does not allow read from stdin |
| CSCsd98887 | Cisco IOS | SP Memory Leak In mls-msc Process |
| CSCse00115 | Cisco IOS | mcast egress replication -- Wrong output interface index for msc |
| CSCse00135 | Cisco IOS | Initial few sweep ping packets fail for MLPoMPLS |
| CSCse00284 | Cisco IOS | ION Code crashes active sup under heavy stress and show proc cpu cmd |
| CSCse01998 | Cisco IOS | All vlans in FWSM gets removed after doing no fire mod 9 vlan-gr 11 |
| CSCse08044 | Cisco IOS | Netflow Export produced wrong flow record on cache expiration . |
| CSCse09852 | Cisco IOS | Low PPPoEoQ Call Rates with Netflow config on VT intf |
| CSCse11333 | Cisco IOS | Native IOS does not syslog thermal warnings from IDSM-2 Cat6k card. |
| CSCse11794 | Cisco IOS | MPB+QoS: Observe SIP1crash with scaled atm bridged vc . |
| CSCse12195 | Cisco IOS | 6816: Interface 3/4 flapping when interface 3/1 is not connected |
| CSCse12314 | Cisco IOS | Synguard rate limits tcp probes syn packets |

| Identifier | Technology | Description |
|---|---|---|
| CSCse14269 | Cisco IOS | Failed to obtain ident counters for stats update |
| CSCse14548 | Cisco IOS | DHCP SNOOPING support for receiving giaddr nonzero in untrusted port |
| CSCse15728 | Cisco IOS | VPNSM does not perform invalid spi recovery in vrf mode |
| CSCse15947 | Cisco IOS | 20 seconds of traffic loss after test crash 9 on active SP |
| CSCse16512 | Cisco IOS | Egress Queuing on WS-6148-21AF broken |
| CSCse16923 | Cisco IOS | 5850: IOS upgrade issue in handover split mode |
| CSCse17175 | Cisco IOS | Line down on some serilal interfaces for Chann STM-1 SMI PA |
| CSCse19351 | Cisco IOS | VTI-FVRF:table_id shuld only be consumed when crypto VRF is configured . |
| CSCse19732 | Cisco IOS | Not able to apply policy on a port -which is earlier part of l3 port-cha |
| CSCse19848 | Cisco IOS | Multicast / Broadcast SNMP counters aren't populated for some interfaces |
| CSCse27836 | Cisco IOS | LACP MiniLink Portchannel flaps though hotstandby ports exist |
| CSCse29001 | Cisco IOS | ISIS did not update when encap frame-relay on POS SPA of SIP-400 |
| CSCse29419 | Cisco IOS | Need SNMP support for traffic counters given by 'show vlan counters' |
| CSCse30293 | Cisco IOS | Inbound SA  not setup correctly |
| CSCse31973 | Cisco IOS | NF double counts packets when span is configured. |
| CSCse33257 | Cisco IOS | Intf Flap causes memory Hog in mls-msc on DFC installed Sup720 system |
| CSCse33395 | Cisco IOS | HSRP track interface in down state in ITASCA though active on SUP |
| CSCse33420 | Cisco IOS | LACP: config for some other port-channel gets removed on bundling ports |
| CSCse33488 | Cisco IOS | DS1: Back to back connectivity not successful between T1/E1 SPA-PA |
| CSCse33543 | Cisco IOS | VSEC: IKE SAs stays in MM_KEYEXCH state -RSA signature |
| CSCse34615 | Cisco IOS | Radius Acct on-off messages are dropped by Vserver |
| CSCse34697 | Cisco IOS | crypto injected route points to wrong interface . |
| CSCse35278 | Cisco IOS | VPNSM drops transit NAT-T packets |
| CSCse37364 | Cisco IOS | traceback @ hal_get_dist_job on toggling mmls |
| CSCse37587 | Cisco IOS | DHCP snooping in conjunction with VRF breaks DHCP |
| CSCse39956 | Cisco IOS | VPLS:UCODE:Replication broken when CW followed by NO_CW VC |
| CSCse41480 | Cisco IOS | cos vlan priority is not preserved for MPLS traffic over EoMPLS tunnel |
| CSCse43709 | Cisco IOS | supw nmi support |
| CSCse47430 | Cisco IOS | Need boundry check in heartbeat_create_recv_info |
| CSCse47638 | Cisco IOS | SP and linecard CPUHOG tracebacks at earl7_read_adj_entry when flap link |
| CSCse47732 | Cisco IOS | No support for DS3-MIB for channelized STM1 SPA . |
| CSCse47811 | Cisco IOS | Guard output does not reach GRE tunnels on SUP-720 |
| CSCse48657 | Cisco IOS | config sync will reset standby when no EEM policy only on active |
| CSCse49072 | Cisco IOS | sierra: Online diag status for SIP spa modules Unknown / Not Applicable |
| CSCse49388 | Cisco IOS | Tunnel int fails to receive traffic when links of a diff tunnel shut . |
| CSCse49846 | Cisco IOS | Sierra: Convergance issues; avoid snding RPF-chg followed by sc-delete . |
| CSCse51577 | Cisco IOS | Sup2/MSFC2: Memory leak at Dead/FM VMR chunk when pasting in NAT config |

| Identifier | Technology | Description |
|---|---|---|
| CSCse53002 | Cisco IOS | Memory leak in IPSEC key engine process at kmi_malloc_num_sas |
| CSCse53090 | Cisco IOS | After console timeout, access can be done to standby console. |
| CSCse54768 | Cisco IOS | CASA traffic not CEF switched |
| CSCse56921 | Cisco IOS | GTP SLB Reloads at the time of session/sticky creation in multiple vserv |
| CSCse59209 | Cisco IOS | Seeing spurious mem trace back when change etherchannel mode to pagp |
| CSCse59363 | Cisco IOS | Crash with an inband/out-of-band channel deadlock detection |
| CSCse59777 | Cisco IOS | WLSM: CPUHOG on L3mm process |
| CSCse59865 | Cisco IOS | ESM20G/SIP600:Router crashes at vlan_if_get_data on bootup w/ 100 subf |
| CSCse60601 | Cisco IOS | Standby Sup crash due to ACLDeny bug in TYCHO |
| CSCse60667 | Cisco IOS | mfiSlaBasic-bat regression cores on show ip cef with feature lfd summary |
| CSCse61252 | Cisco IOS | ION : reset reason displayed incorrectly in show version |
| CSCse61387 | Cisco IOS | After LC is removed, show policy-map control-plane still show LC counter |
| CSCse65726 | Cisco IOS | command no tacacs-server admin resets router |
| CSCse66269 | Cisco IOS | ION free memory dropping during mcast failovers but no process leaking |
| CSCse69360 | Cisco IOS | CLI output from show running-config <spa module number> is broken |
| CSCse69713 | Cisco IOS | Redirect traffic punted to software when all CEs in the group are lost |
| CSCse69748 | Cisco IOS | CLI for IMAP retcode in CSG refunding is broken |
| CSCse70423 | Cisco IOS | change WS-X6708-10GE  default behavior for non-E chassis |
| CSCse72235 | Cisco IOS | LAC crash when fragmenting ingress PPPoA and labelled in egress |
| CSCse73539 | Cisco IOS | c7600 - crash of active sup720 after inserting a second one |
| CSCse75904 | Cisco IOS | VPNSM: periodic accounting is still sent for disconnected vpn users |
| CSCse77196 | Cisco IOS | Parser truncates pre-shared keys in keyring when line length > 256 bytes |
| CSCse77427 | Cisco IOS | 7600 H-VPLS performance issues using SIP-600 and 10G SPA |
| CSCse77768 | Cisco IOS | Mac learning missing some MAC when traffic sent from MPBE to VPLS core |
| CSCse78548 | Cisco IOS | LSR adds incorrect label stack (label 1) |
| CSCse81638 | Cisco IOS | Output stuck on WS-X6524-100FX-MM module |
| CSCse82589 | Cisco IOS | LSR mishandles packets with router-alert label |
| CSCse83031 | Cisco IOS | memory leak reported with Eompls cfg with EFP  xconnect child trees |
| CSCse84226 | Cisco IOS | AToM: vc state UP under sh connection when MTU is mismatched |
| CSCse84602 | Cisco IOS | Error messages from Standby Sup when configuring OSM card channelization |
| CSCse84695 | Cisco IOS | Standby supervisor may crash when configuring osm card past FREEDM limit |
| CSCse86602 | Cisco IOS | Cat6500 IOS does not set correct portAdminSpeed |
| CSCse87210 | Cisco IOS | Enable service cards to operate in crossbar mode with Dist Etherchannels |
| CSCse87417 | Cisco IOS | FlexLink : ARP frames w/ known opcodes cause interop issues. |
| CSCse87618 | Cisco IOS | cRTP and Interleave doesnt work together on Virtual-Template Interface. |
| CSCse88171 | Cisco IOS | PA-MC-8TE1+: cRTP compression failure |
| CSCse88708 | Cisco IOS | Early stop of Bert test on OSM-1CHOC12/T1-SI produces error |

| Identifier | Technology | Description |
|---|---|---|
| CSCse89636 | Cisco IOS | LFD-3-INVINSTALLER LSD-3-LABEL msgs and tracebacks when PRE2 -PRE3 ISU |
| CSCse90572 | Cisco IOS | FIB TCAM exception related enhancements |
| CSCse90586 | Cisco IOS | upon low mem crypto kmi crashed with double-free pyld . |
| CSCse91987 | Cisco IOS | slbConnectionTable objects are  not getting populated on snmp query |
| CSCse95888 | Cisco IOS | E5 FE SPA interface bandwidth changes when the remote interface is shut |
| CSCse98354 | Cisco IOS | SIP-200: SYNC FAILED not initialized. Interfaces up/down. |
| CSCse98369 | Cisco IOS | class-default bandwidth percent 100% - SPA ATM fails |
| CSCse98570 | Cisco IOS | 802.1q subinterfaces have no ifIndex on SUP32 |
| CSCse98692 | Cisco IOS | 12.2SX code not showing int trust state in sh mls qos cmd |
| CSCse98795 | Cisco IOS | bus error while printing access-list |
| CSCsf03566 | Cisco IOS | Memory corruption crash trying to free unassigned block |
| CSCsf03730 | Cisco IOS | interface remains down even after E1 level local loopback on STM1 |
| CSCsf04112 | Cisco IOS | Getting ifPhysAddress changes mac-address of SPA-2X1GE |
| CSCsf05390 | Cisco IOS | CPU HOG @ hwidb_iftype_unlist followed by router crash. |
| CSCsf07232 | Cisco IOS | tclsh stdio operations do not output to current terminal |
| CSCsf08368 | Cisco IOS | Prevent NBAR configuration on non-FlexWAN interfaces |
| CSCsf08419 | Cisco IOS | EIGRP memory leak in registry_ion.c when neighbor flaps. |
| CSCsf08502 | Cisco IOS | event_reqinfo event_pub_sec/event_pub_msec missing for event_none events |
| CSCsf08803 | Cisco IOS | event snmp may wrongly triggered when using type increment |
| CSCsf09219 | Cisco IOS | SYS-2-NULLCHUNK messages/Traceback @ipflow_create_template in netflow |
| CSCsf10116 | Cisco IOS | Reflexive ACL not getting Sw Installed. |
| CSCsf10203 | Cisco IOS | MLD gces not freed even after MLD leaves and L3 traffic stopped |
| CSCsf10605 | Cisco IOS | crypto session count incorrect after ungraceful disconnect |
| CSCsf11098 | Cisco IOS | 12.2(SRA) releases report errors trying to FPD upgrade SPA-2X1GE-V2 SPA |
| CSCsf11639 | Cisco IOS | WS-X6148-FE-SFP interface counter increments even if the link is down |
| CSCsf11787 | Cisco IOS | EARL bus idle error occurs when the switching bus stall occurs |
| CSCsf13044 | Cisco IOS | MVPN: Bidir mroute OIF missing - pim joins not received from MDT tunnel |
| CSCsf14994 | Cisco IOS | SIP1-ChOC3:Some of the MLP links wont ping, if deleted & configred again |
| CSCsf15527 | Cisco IOS | ION: Reset Reason Does Not Change on Normal Reload |
| CSCsf17163 | Cisco IOS | TCAM mask/entry resource not released after conf/unconf pacl |
| CSCsf17739 | Cisco IOS | Sup720 SVI does not show multicast traffic rate |
| CSCsf18752 | Cisco IOS | mls ip slb search wildcard rp breaks gtp slb if 2 sfarms are confgd |
| CSCsf20751 | Cisco IOS | FlowControl inconsistency between Po and gig interfaces after SW upgrade |
| CSCsf21629 | Cisco IOS | physical links on neighboring switch flap after first SSO |
| CSCsf22364 | Cisco IOS | PortLoopbackTest failed for OC-12 POS SPA on bootup with 26th Aug Image |
| CSCsf22829 | Cisco IOS | EEM Interface event detector sets old value to the sample value |
| CSCsf23115 | Cisco IOS | SUP720 does not recognize FAN2 after one of fans failed. . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsf25240 | Cisco IOS | Qos queue-limit warning message on bootup |
| CSCsf26400 | Cisco IOS | Cat6000 may not power up all POE devices after reload |
| CSCsf27493 | Cisco IOS | Ports on WS-6724-SFP with GLC-T adapters don't come up |
| CSCsf28708 | Cisco IOS | TestQos failed on SIP-600 on 12.2SRA |
| CSCsf31458 | Cisco IOS | R3Vail: SupW image - entPhysicalTable is not SSO aware. . |
| CSCsf32012 | Cisco IOS | Fix CSCsc77521 for 6748/DFC |
| CSCsf96390 | Cisco IOS | C7600:subinterface ifIndex is disappearing after reload for PA-STM1 |
| CSCsf96476 | Cisco IOS | Router Crash when enabling BFD on ISIS- bfd_intf_addr_change_walker |
| CSCsf96980 | Cisco IOS | No ipv mrib clients established after second SSO switchover, no HW switc |
| CSCsf97682 | Cisco IOS | Last port of T3/E3 SPA connected back to back does not ping |
| CSCsf98341 | Cisco IOS | UDLD failed to receive PDU when linked to L3 port. |
| CSCsf98713 | Cisco IOS | PVST/MST compabitility fix for TELUS |
| CSCsf98858 | Cisco IOS | AB76: BFD echo mode fail detection time is much longer than async mode |
| CSCsf99460 | Cisco IOS | SUP720 cannot disable link-status traps for EOBC0/0 interfaces |
| CSCsg00173 | Cisco IOS | v4 Sparse/SSM traffic when src is in PVLAN src port/DFC is not routed |
| CSCsg00845 | Cisco IOS | 'no logging event link-status' is lost after reload |
| CSCsg01644 | Cisco IOS | EEM debug event manager tcl cli sent to the console, script may crash |
| CSCsg02241 | Cisco IOS | SUP720/SUP32 NAT translates incorrectly |
| CSCsg02391 | Cisco IOS | PORT_SECURITY-SP-2-INELIGIBLE error after module reset |
| CSCsg02605 | Cisco IOS | Rapid reboot does not work |
| CSCsg03739 | Cisco IOS | cat6k with vpnsm several possible crypto ikmp leaks . |
| CSCsg04681 | Cisco IOS | MPLS tunnel recir failed after tunnel is taken over by vpnspa |
| CSCsg06577 | Cisco IOS | 'Desc ordr internal vlan allocation' brings up sup with major diag error |
| CSCsg07525 | Cisco IOS | Periodic (30sec) traffic loss/dup over dis port-cha due to wrong RBH |
| CSCsg07765 | Cisco IOS | Sierra: scp_fpoe_req: memory allocation error, subopcode=10, count=9 |
| CSCsg07870 | Cisco IOS | crash seen on switchover at pf_redun_sync_port_asic_on_swover . |
| CSCsg08200 | Cisco IOS | JQL: Bootup diagn for LC detect major failure after RPR swover . |
| CSCsg08304 | Cisco IOS | JQL: UDLD failure detected on neighbor switch after RPR switchover . |
| CSCsg09757 | Cisco IOS | MP(Maintenance Pack) information missing in the MIB . |
| CSCsg10075 | Cisco IOS | 'show policy-map i/f' on --more-- prompt blocks MQC database updates |
| CSCsg10159 | Cisco IOS | Successive Default route ctrl fails on different link but on same router |
| CSCsg10531 | Cisco IOS | Packet loss ratio is more than tolerance under dynamic stress |
| CSCsg11616 | Cisco IOS | iprouting restart crashes Sup due to Block overrun at 5E64940 (red zone |
| CSCsg12887 | Cisco IOS | mcast over gre - tunnel key crashes the box even at low rate traffic(20p |
| CSCsg13828 | Cisco IOS | fh_fd_timer.proc crashed without any special trigger |
| CSCsg16272 | Cisco IOS | Catalyst6500 LinkDown snmp trap does not generate while performing OIR . |
| CSCsg16425 | Cisco IOS | show ip slb reals command displays huge connections value |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg16964 | Cisco IOS | Sup32 crashes with 23rd image tb@_shmwin_error |
| CSCsg18080 | Cisco IOS | Router crashes on trying to get snmp counters |
| CSCsg23979 | Cisco IOS | Crashes in iprouting.iosproc produce no tracebacks |
| CSCsg24215 | Cisco IOS | SNMP linkdown traps not generated |
| CSCsg24609 | Cisco IOS | Whitney: snmp CISCO-L2-CONTROL-MIB getmany errors . |
| CSCsg24971 | Cisco IOS | IPC Failure message on WS-X6816-GBIC while displaying netflow entries |
| CSCsg25416 | Cisco IOS | flash information is missing from show hardware output in ION |
| CSCsg27123 | Cisco IOS | Learning not disabled on SPAN dest without learning option |
| CSCsg27783 | Cisco IOS | DFC tcam wrongly progged when policy map is appld with VACL,Reflex. acl |
| CSCsg28959 | Cisco IOS | rwindex = 0xFFFF on the non PI causing all mcast traffic to be dropped |
| CSCsg30355 | Cisco IOS | OIR of redundant sup w/ CatOS crash the Cat6500 System running IOS |
| CSCsg32319 | Cisco IOS | Probe connections not cleaned up when access/vrf is configured . |
| CSCsg34141 | Cisco IOS | Secure mac learnt on non secure port creates a static entry |
| CSCsg35506 | Cisco IOS | JQL: port-channel member in suspend due to flowcontrol mismatch . |
| CSCsg36726 | Cisco IOS | Bonham parity errors may cause packet loss on a 7600-SIP-400 module. |
| CSCsg37435 | Cisco IOS | ifIndex missing for 802.1Q vLAN subif after GigEth card OIR . |
| CSCsg37484 | Cisco IOS | Bus Error in crypto_map |
| CSCsg37644 | Cisco IOS | IOS SLB does not work on 7600 if Client is behind MPLS cloud |
| CSCsg38231 | Cisco IOS | 'crypto eng gre vpnblade' cmd does make the tunnels to be accelerated by |
| CSCsg38618 | Cisco IOS | Session to a 24 bit address fails on WiSM |
| CSCsg38930 | Cisco IOS | 7600 SPA-IPSEC-2G - Multicast data is not forwarded through GRE Tunnel |
| CSCsg39665 | Cisco IOS | CPP: Add MIB support for Control-Plane interface |
| CSCsg39754 | Cisco IOS | DHCP snooping redirect ACL permits more than just bootpc and bootps port |
| CSCsg40267 | Cisco IOS | SPA-OC192POS-XFP reports voltage outside of nominal range |
| CSCsg40391 | Cisco IOS | Dot1x: Port config on authenticated port changed after linecard reset |
| CSCsg40401 | Cisco IOS | SUP32 unstable to communicate with all neighbors after reload. |
| CSCsg41552 | Cisco IOS | Module fails to come online first time after reset |
| CSCsg42860 | Cisco IOS | ACE-R6: Back Plane Link RESET to 8 GIG after SUP Switchover |
| CSCsg43284 | Cisco IOS | ISAKMP non-first frag doesn't reach RP from VPNSPA |
| CSCsg46087 | Cisco IOS | Packet dropped at ocpu for packet size greater than 1461 |
| CSCsg49395 | Cisco IOS | %BIT-SP-4-OUTOFRANGE: bit is not in the expected range |
| CSCsg51230 | Cisco IOS | VS2: MLS multicast operating state is IDLE, after SSO switch over |
| CSCsg51724 | Cisco IOS | cbQosCMDropPkt stays at 0 while CLI counters shows positive values |
| CSCsg51811 | Cisco IOS | OER BGP Inbound advert incorrectly modifies all inside prefix adverts . |
| CSCsg52355 | Cisco IOS | RHI  Injected routes  lost after SUP switchover |
| CSCsg53461 | Cisco IOS | Service Internal incorrectly required for Purge Interface Command |
| CSCsg53526 | Cisco IOS | Some packets to vip are denied by inbound acl after server nat |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg53550 | Cisco IOS | EOU commands cannot be enabled on sub-interface |
| CSCsg55237 | Cisco IOS | L2 flooding stops when new MAC address entries are learnt |
| CSCsg55315 | Cisco IOS | Packets duplicated out of Gig1/1 when SPAN Monitor session enabled |
| CSCsg56625 | Cisco IOS | E3 LC continutes crash by receive corrupt  tag packets ttl=1 |
| CSCsg58587 | Cisco IOS | On 7604 snmp output counters for vlan are counted twice |
| CSCsg58854 | Cisco IOS | SPA Ethernet HC 64-bit SNMP counters wrap after reaching 2^32 |
| CSCsg61773 | Cisco IOS | MMLS: Egress mode, OIF inconsistent between SP/RP, traffic blackholed |
| CSCsg61795 | Cisco IOS | RLB should not re-use a session when no session-id has been set |
| CSCsg62154 | Cisco IOS | 18SXF7: ltl_alloc_index_at: T/Bs are seen after multiple switchover |
| CSCsg64170 | Cisco IOS | SSO switchover causes service module to appear down for 10-30 secs . |
| CSCsg64306 | Cisco IOS | %MCAST-SP-6-L2_HASH_BUCKET_COLLISION |
| CSCsg64327 | Cisco IOS | Tunnels go down with multicast traffic in global vrf mode. |
| CSCsg66543 | Cisco IOS | CISCO-SWITCH-ENGINE-MIB, inconsistent L3 stats between CLI and SNMP. |
| CSCsg67551 | Cisco IOS | LDP session starts to flap after graceful-restart on switchover |
| CSCsg68740 | Cisco IOS | FRR is not triggered when cable is removed from a POS SPA/OSM LC |
| CSCsg68783 | Cisco IOS | ATM SAR hangs when MPLS TE auto-tunnel mesh is cleared |
| CSCsg69081 | Cisco IOS | show crypto ipsec sa should indicate if pfs in use |
| CSCsg69605 | Cisco IOS | Need to reword SYSTEM_CONTROLLER-3-EXCESSIVE_RESET syslog |
| CSCsg69646 | Cisco IOS | 'timer wheel' not running for the tunnel . |
| CSCsg70932 | Cisco IOS | ESCORT: router crashes with QoS on and traffic running |
| CSCsg72398 | Cisco IOS | SLB:Packets getting process switched w/ multiple UDP Vservers |
| CSCsg72678 | Cisco IOS | TCAM entries not displayed for DFC card after OIR . |
| CSCsg73179 | Cisco IOS | bi-dir mls rp doesnt get updated after a change in topology . |
| CSCsg73688 | Cisco IOS | Whitney,SNMP,CBQOS,enahnce cbQosPoliceCfgRate64 to support 10G int. |
| CSCsg75132 | Cisco IOS | REDUNDANCY-3-IPC: cannot open standby port session in use |
| CSCsg77142 | Cisco IOS | Memory leak in Cat6k SNMP Trap process |
| CSCsg77629 | Cisco IOS | Need to add a command to turn off/on FEFI |
| CSCsg79810 | Cisco IOS | The MPLS MTU is overruled by the ip mtu on ATM interface |
| CSCsg80948 | Cisco IOS | Uneven load-sharing for 4-path ECMP case |
| CSCsg85046 | Cisco IOS | 7600 router with SPA-4XOC48POS/RPR on SIP-600 crashes on bootup |
| CSCsg85415 | Cisco IOS | heartbeat_fatal crash, CPU HOG tracebacks point to SEA |
| CSCsg87228 | Cisco IOS | Serial interface (T1 or E1) NOT working with Crypto Connect |
| CSCsg87235 | Cisco IOS | EEM config prevents telnet connection |
| CSCsg90190 | Cisco IOS | Software does not limit 96 Ports LC inline Power based on HW Limitation |
| CSCsg91545 | Cisco IOS | ACL TCAM inconsistency seen if ipv6 acl with 2k mask is used . |
| CSCsg92393 | Cisco IOS | SUP720 CEF loadshare algorithm simple mode does not work for IPv4 |
| CSCsg92950 | Cisco IOS | memory corruption overruning oce counter stack |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg92954 | Cisco IOS | Poor Voice Quality over congested Links |
| CSCsg94023 | Cisco IOS | show int status does not show routed port correctly |
| CSCsg94565 | Cisco IOS | PreFrag not works with tun mtu > secure mtu, packet size just > tun mtu |
| CSCsg97755 | Cisco IOS | CMFI Background process produces %SYS-SP-3-CPUHOG |
| CSCsg98045 | Cisco IOS | EEM track event detector missing maxrun option for tcl scripts |
| CSCsg99084 | Cisco IOS | mago: ME-C6524 Tx CRC errors on uplink ports with 100FX SFP . |
| CSCsg99369 | Cisco IOS | Isakmp processes TV attributes as TLV |
| CSCsg99872 | Cisco IOS | VPNSM: IPSEC accounting (start/stop) not sent under some conditions |
| CSCsg99877 | Cisco IOS | AToM: load balancing not happening on the core links |
| CSCsg99914 | Cisco IOS | sip-200 power-cycles after BGP flap (not responding to keepalive) |
| CSCsh02514 | Cisco IOS | MCAST: rpf null for (S,G), process switched on shared tree |
| CSCsh05800 | Cisco IOS | Mcast egress replication - VDB is not updated on L3 PO subinterfaces |
| CSCsh06605 | Cisco IOS | Modular IOS Kernel Release |
| CSCsh11498 | Cisco IOS | %SM-4-BADEVENT: Event rt_reg_ok is invalid for the current state wait |
| CSCsh13947 | Cisco IOS | EoMPLS: Router crashes @ ipv4fib_pas_frag_pak |
| CSCsh15366 | Cisco IOS | Ether SFP/XFP SPAs : Peer link up incorrectly |
| CSCsh15864 | Cisco IOS | Interfaces follow no logical order in sh mls qos ip output |
| CSCsh16213 | Cisco IOS | Disabling MLDsnooping does not clean special MACs 3333.0000.0016, 3333.0 |
| CSCsh17979 | Cisco IOS | Ports PWR_DENY not enough system PWR/chassis BackPlane PWR (Not Real) |
| CSCsh20211 | Cisco IOS | 'Complete' diags fail TestNetflowInlineRewrite test on Service Modules |
| CSCsh20354 | Cisco IOS | client does not receive mode config data |
| CSCsh20950 | Cisco IOS | 18SXF8: PRBS support needs to be disabled on the Malabar8 module |
| CSCsh21371 | Cisco IOS | Catalyst 6500 msfc last reload date not reset properly after reload |
| CSCsh22835 | Cisco IOS | Major Error is seen with module 6 after swithover in rpr mode. . |
| CSCsh23961 | Cisco IOS | Multicast netflow not working for Vlan interface (SVI) |
| CSCsh25976 | Cisco IOS | C2W1: SSO sync issue with PSFANINCOMPAT & PSFANFAIL sensor . |
| CSCsh27094 | Cisco IOS | SSO: VPN Spa got reset twice when subslot x/1 present |
| CSCsh27234 | Cisco IOS | Packet drop occurs at the moment uRPF applied |
| CSCsh28014 | Cisco IOS | After unconfig MPLS, seen %SCHED-CFC8-3-UNEXPECTEDEVENT & Traceback |
| CSCsh29863 | Cisco IOS | New active crashes after switchover in rpr mode . |
| CSCsh30617 | Cisco IOS | EEM software forced crash when unregistering an applet |
| CSCsh31287 | Cisco IOS | tunnel mcast adj shows src mac is all zeros |
| CSCsh31306 | Cisco IOS | T1 serial o/p drops / no QOS drops - flexwan - T1 multichannel PA. |
| CSCsh33128 | Cisco IOS | MMLS/MVPN: Partial SC internal vlan not included in (*,G) |
| CSCsh33518 | Cisco IOS | STP information is not in sync with Active . |
| CSCsh33770 | Cisco IOS | contrl vlan not set; zamboni remains in initializing state . |
| CSCsh34872 | Cisco IOS | With mls mpls recirc configd primary internal vlan has vpn-num . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsh35311 | Cisco IOS | Proxyacl downloaded from the ACS cause spurious memory access |
| CSCsh35600 | Cisco IOS | Change CSCsc81300 behavior for deny log ACEs |
| CSCsh36377 | Cisco IOS | crypto connect cmd not updated in standby RP for ATM subif . |
| CSCsh37008 | Cisco IOS | Need to enable Malabar8 in WS-C6509-NEB-A chassis with one fan . |
| CSCsh37272 | Cisco IOS | BFD cpu pegs, invalid element for addition, possible crash |
| CSCsh37276 | Cisco IOS | Switch crashed @ fm_ipv4_intf_nde_req_process |
| CSCsh38443 | Cisco IOS | Removing associated vlan would trigger the mac-add to get purge every 5m |
| CSCsh38737 | Cisco IOS | Flexwan with PA shows incorrect serial int count on sh ver after reload. |
| CSCsh39318 | Cisco IOS | 10K / PRE-2 crashes at %MROUTE-4-ROUTELIMIT |
| CSCsh42857 | Cisco IOS | MPLS-TE: After tunnel reoptimization the tunnel label is not updated |
| CSCsh45258 | Cisco IOS | delay execution of redundancy force switchover in case stdby nrd . |
| CSCsh45949 | Cisco IOS | SA's are created by the crypto engine in the wrong subslot |
| CSCsh48439 | Cisco IOS | Sup4:Jagger is not supported |
| CSCsh48947 | Cisco IOS | PWR_DENY Port 47/48 on each LC max PWR support  Backplane per LC or VDB |
| CSCsh49043 | Cisco IOS | Output drops in Queue3 after changes in cos-map config on 6148A-GETX . |
| CSCsh49239 | Cisco IOS | After redundancy failover Mcast packets drop for 60-90sec on SUP uplink |
| CSCsh52941 | Cisco IOS | AUTHPROXY:CLI to increase the number of HTTP Proxy process |
| CSCsh53141 | Cisco IOS | IKE SA not getting deleted after clear crypto session |
| CSCsh54325 | Cisco IOS | SIP600/ES20 PXF punt path broken when sup slot is 1 or 2 |
| CSCsh54516 | Cisco IOS | JQL:ModularIOS ~80% ARP Proccess performance degradation compared to IOS |
| CSCsh54951 | Cisco IOS | PBR: TCAM incorectly programmed when match statement is NOT used |
| CSCsh56121 | Cisco IOS | Losing RSA keys on Standby Supervisor after switchover or reload |
| CSCsh59346 | Cisco IOS | allowed number for port-chan interface is not correct for config cli |
| CSCsh61396 | Cisco IOS | R3.8: Hydra module resets during to excessive LCP_FW_ERR Qchip msgs |
| CSCsh61946 | Cisco IOS | Second 6kW DC power supply is shutdown after SSO switch over. |
| CSCsh62565 | Cisco IOS | SSH keys regenerated every hour cause route flaps due to high CPU load |
| CSCsh68327 | Cisco IOS | C6k: rxOversizedPkts counter counts up when link flaps |
| CSCsh68976 | Cisco IOS | memory leak at xcvr_idprom when executing show hw-module all tranceiver |
| CSCsh69601 | Cisco IOS | SNMP poll output byte counters are inaccurate in 12.2(33)SRA1 |
| CSCsh70393 | Cisco IOS | no output from sh env voltage command |
| CSCsh72111 | Cisco IOS | mls rate-limit layer2 ip-admission shouldn't be enabled by default |
| CSCsh73935 | Cisco IOS | RP crash with SNMP get to ciscoMvpnMrouteMdtEntry |
| CSCsh74322 | Cisco IOS | rp fails bootup when reload installed image with 42 patch in 1 tar ball |
| CSCsh74385 | Cisco IOS | EEM fails to register with the redundancy framework (RF) |
| CSCsh74417 | Cisco IOS | crash in c10k_remote_crash_interrupt |
| CSCsh76923 | Cisco IOS | Memory Corruption or bus error crash on cat6k running NAT . |
| CSCsh77220 | Cisco IOS | SSO failover causes certain configs being removed . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsh80993 | Cisco IOS | VTP Domain Name is not updated on show cdp neighbor detail after rpr sw |
| CSCsh83109 | Cisco IOS | HapiEchoTest fails on SPA-IPSEC-2G when reset. |
| CSCsh83559 | Cisco IOS | Modular IOS: memory leak in xdr_reference |
| CSCsh85833 | Cisco IOS | VACL display sequence does not match between show run and show start |
| CSCsh87819 | Cisco IOS | Traffic-class passive thruput not measured correctly |
| CSCsh92031 | Cisco IOS | Sierra: Standby RP crashed at auth_proxy_posture_clear_nacl |
| CSCsh94105 | Cisco IOS | force supervisor to rommon in a cleaner way |
| CSCsh94882 | Cisco IOS | Unity client not initiating mode config should be rejected |
| CSCsh94940 | Cisco IOS | Supervisor crash by memory corruption (BADFREEMAGIC) in free block . |
| CSCsh95304 | Cisco IOS | unequal weight on multiple paths is not correctly calculated |
| CSCsh98208 | Cisco IOS | PIM Snooping strips out Prune List in a (*,g) Join (s,g) RPT prune msg . |
| CSCsh98849 | Cisco IOS | SIERRA: Active and stby SP and active RP crashed@rf_proxy_fatal_error |
| CSCsi00136 | Cisco IOS | IKE does not process more than 2 NAT-D payload |
| CSCsi00173 | Cisco IOS | Bus error at crypto_ipsec_unlock_peer . |
| CSCsi00377 | Cisco IOS | Exit Mismatch when application & prefix with common dst have diff policy |
| CSCsi00706 | Cisco IOS | Sierra: upon fib tcam exception to use ratelimiter and not reload |
| CSCsi00712 | Cisco IOS | Connected ipv4 routes for WAN interfaces missing on reload |
| CSCsi02033 | Cisco IOS | 7600 - creating a new dot1q subinterface breaks eompls vc |
| CSCsi04335 | Cisco IOS | Web Auth performance numbers are not as expected. |
| CSCsi09388 | Cisco IOS | VPNSM SA deleted by idle timeout |
| CSCsi10219 | Cisco IOS | receive side sip1 crashes when rtp traffic is sent for hw MLP + CRTP . |
| CSCsi10945 | Cisco IOS | Http Auth-proxy with OTP does not display token/SNK challange |
| CSCsi11382 | Cisco IOS | Diags failing for NAM module. Module powered down |
| CSCsi12289 | Cisco IOS | FWSM Does Not Display Correct Timezone for DST |
| CSCsi14145 | Cisco IOS | runt counter not implemented correctly |
| CSCsi14965 | Cisco IOS | Need to remove compression cli from cwpa/cwtlc if not supported |
| CSCsi15191 | Cisco IOS | BOM messages observed while activation of rollback on stndby supervisor |
| CSCsi26184 | Cisco IOS | possible fix for CSCsh71274 - improper pak subblock free in ttlexp path |
| CSCsi32436 | Cisco IOS | SNMP set in CISCO-VLAN-MEMBERSHIP-MIB does not mark config changed |
| CSCsi40628 | Cisco IOS | Dual RSPAN session causes loop between 2 6500 chassis . |
| CSCsi42517 | Cisco IOS | SRB Crashes when upgrading from SXF to SRB with SLB stateful config |
| CSCsi42769 | Cisco IOS | VPNSPA crashes with large certificates (PKI) . |
| CSCsi45454 | Cisco IOS | ENH to allow traffic to be forwarded with packet-buffer action ignore |
| CSCsi46469 | Cisco IOS | SNMP:loop in cbqosmib on 7609 12.2(33)SRA2 |
| CSCsi46861 | Cisco IOS | %MFI-3-REDISTMGR: Redistribution Manager: tracebacks following SSO |
| CSCsi48975 | Cisco IOS | system crash due to Invalid memory action (malloc) at interrupt level |
| CSCsi49520 | Cisco IOS | After SSO, no EOBC buffer available., system cannot recover . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsi51649 | Cisco IOS | RP crashes@fm_send_inband_install_message+21C in many cases with NAT |
| CSCsi52209 | Cisco IOS | 7600-sip-600 crash at PXF-DFC1-2-FAULT: T0 OHB Exception: SLIP FIFO full |
| CSCsi54333 | Cisco IOS | RP Inlet & Outlet temperatures displayed as N/A on Sup32 |
| CSCsi55626 | Cisco IOS | SP hung/RP crashed after mld hosts left from 200-vlan |
| CSCsi56793 | Cisco IOS | Tracebacks seen and Unexpected call: sp_power_mgmt_led() on DFC wan card |
| CSCsi60125 | Cisco IOS | Hosts receive TCP RST due to incorrect NAT translation on cat6k . |
| CSCsi60472 | Cisco IOS | Change default packet-based NF sampling rate to 16 seconds |
| CSCsi64204 | Cisco IOS | SXF:SIP400:ATMSPA Noticeable delay in output of show int atm command |
| CSCsi69234 | Cisco IOS | BFD SM: transition state from Init to Up if recv bfd init packet |
| CSCsi70920 | Cisco IOS | Return traffic doesn't trigger EOU when ip admission on two interfaces |
| CSCsi72758 | Cisco IOS | clear multicast traffic not get to vpnspa in crypto connect mode . |
| CSCsi74360 | Cisco IOS | packet loops between icpu and ocpu while sending clear mcast traffic |
| CSCsi74923 | Cisco IOS | Traceback on changing netflow flowmask |
| CSCsi76192 | Cisco IOS | r3:show wism status not populated until standby up after SSO |
| CSCsi76936 | Cisco IOS | Crash in GLBP if debug is enabled and it rcvs pkt from unknown group |
| CSCsi77983 | Cisco IOS | RP crashed ipflow_pak_pre_check on shutdown the trunk port |
| CSCsi86691 | Cisco IOS | IOS: BR crashes when it learns OER prefixes via dynamic PBR |
| CSCsi88920 | Cisco IOS | MLD rcvr in SVI stops receiving v6 mcast trffc if another rcvr leaves |
| CSCsi90011 | Cisco IOS | User Auth after Machine Auth causes dot1x security violation |
| CSCsi93683 | Cisco IOS | BFD sessions cannot be removed after creating the maximum number allowed |
| CSCsi94863 | Cisco IOS | New xenpak background task . |
| CSCsi97311 | Cisco IOS | subinterfaces are down in OER even if they are actually up . |
| CSCsi98993 | Cisco IOS | Block FPD for Intel SPROM based ATM SPAs |
| CSCsj01310 | Cisco IOS | Modular-IOS: TCP probes are not working with VRF |
| CSCsj04905 | Cisco IOS | IOS-SLB: FWLB sticky config not get removed |
| CSCsj07935 | Cisco IOS | %CONST_DIAG-SP-2-HM_MOD_RESET:Failed TestFabricCh0Health . |
| CSCsj09249 | Cisco IOS | OER PFR MC crash: divide by 0 crash in oer_br_update_iface_counters |
| CSCsj16292 | Cisco IOS | DATACORRUPTION-1-DATAINCONSISTENCY: copy error |
| CSCsj18014 | Cisco IOS | Caller ID string received with extra characters |
| CSCsj19019 | Cisco IOS | Netflow entries not installed for wccp GRE |
| CSCsj25470 | Cisco IOS | EEM hostnames over 20 characters causes CLI actions to hang |
| CSCsj27811 | Cisco IOS | EOBC buffer leak caused by CMM module . |
| CSCsj40695 | Cisco IOS | EEM: Incorrect TCL event registration string can hang or crash device |
| CSCsj46607 | Cisco IOS | RPF showing up on enabled and disabled check |
| CSCsj53663 | Cisco IOS | EEM: RP crashed at fh_fd_syslog_event_match |
| CSCsj58287 | Cisco IOS | 7600-SSC-400 crashes on reload |
| CSCsj59997 | Cisco IOS | VTI tunnel: Arp for tunnel destination instead next hop. |

| Identifier | Technology | Description |
|---|---|---|
| CSCsj60182 | Cisco IOS | IPSEC Tunnels not coming up in transport adjency mode |
| CSCsj65189 | Cisco IOS | Traffic stops over EOM ckt after SSO and followed by TE FRR cutover |
| CSCsj65755 | Cisco IOS | Packet loss with SPI NOT Available message during rekey . |
| CSCsj82051 | Cisco IOS | Cachelines not invalidated on ICPU in error case . |
| CSCsk09302 | Cisco IOS | CDP packets not received on WS-6704-10GE/CFC links with MLS QoS enabled |
| CSCso08224 | Cisco IOS | WS-X6148-45AF port link takes 8 or more seconds to come up |
| CSCuk56305 | Cisco IOS | no mpls ip propagate-ttl forwarded is configured by default |
| CSCuk57037 | Cisco IOS | IGMP: crash at at ../ipmulticast/igmp.c:3162 |
| CSCsb89463 | Content | WCCP doesn't redirect packets with 'ip cef' enabled |
| CSCsc72066 | Content | MNLB - incorrect affinities installed |
| CSCsc94191 | Content | WCCP does not GRE Redirect TCP FIN packet that would fragment |
| CSCsd20327 | Content | WCCP going up/down |
| CSCse29465 | Content | CASA traceback routing agent in  process causing CPUHOG |
| CSCse45427 | Content | debug ip casa packet displays incorrect values |
| CSCse76405 | Content | CASA wildcard updates dropped |
| CSCsg30875 | Content | wccp blocking telnet to router |
| CSCsh98343 | Content | WCCP redirect-list and mask-acl merge results in wrong redirect info |
| CSCsi05906 | Content | WCCP:appliance failover does not update TCAM adjacency |
| CSCuk60755 | Content | WCCP redirection broken in process switch path |
| CSCuk61396 | Content | WCCP does not interop with NAT/Inspection |
| CSCuk61773 | Content | WCCP: ignore redirect assignment messages with identical content |
| CSCdx62060 | Infrastructure | Interface names made to display full while show int summary done |
| CSCdy11174 | Infrastructure | ciscoFlashCopyTable/ciscoFlashMiscOpTable obj unreadable @ creation |
| CSCee23195 | Infrastructure | Spurious memory access in show ipc queue . |
| CSCee72249 | Infrastructure | snmp-server host only supports 1 host and trap not shown in config |
| CSCef64439 | Infrastructure | PRE takes long time to become STANDBY HOT after switch-over. . |
| CSCef77951 | Infrastructure | excessive processor memory held by IRB/CRB rxtypes |
| CSCeg12652 | Infrastructure | Vrf aware LDP traps fail |
| CSCeg41564 | Infrastructure | Unable to delete snmp-server enable traps sonet from sh run |
| CSCeg62070 | Infrastructure | Tracebacks noticed with Radius configs through HTTP Post |
| CSCeh12411 | Infrastructure | router hangs while executing show runn- |
| CSCeh62781 | Infrastructure | %IPC-5-WATERMARK FAST.control.RIL(2070000.E) seat 2070000 |
| CSCeh74715 | Infrastructure | SNMPv1 should not send traps with counter64 |
| CSCeh88425 | Infrastructure | ip http client password does not survive reload |
| CSCei16552 | Infrastructure | cannot remove snmp-server engineID from running-config |
| CSCei32102 | Infrastructure | Need an option to disable snmp traps for link during switch failover |
| CSCei87744 | Infrastructure | System doesnt count milli-seconds |

| Identifier | Technology | Description |
|---|---|---|
| CSCej57779 | Infrastructure | BGP: some vrf instances are not up on bgp-bpn setup after sys-reload . |
| CSCek32390 | Infrastructure | IP SLA: CPUHOG seen in SAA Event Processor |
| CSCek42751 | Infrastructure | %Error opening system:/running-config (No such file or directory) |
| CSCek46087 | Infrastructure | IPC ack_pending not updated correctly |
| CSCek48739 | Infrastructure | ION config checkpoint SNMP/HTTP handle for sierra branch |
| CSCek55001 | Infrastructure | Dir /recursively with many directories crashes the router |
| CSCek56630 | Infrastructure | race condition in process_sleep_on_timer code |
| CSCek64188 | Infrastructure | Fragmentation fix of CSCek64051 is incomplete |
| CSCek72874 | Infrastructure | Initiator crashes with 500 fvrf and ivrf for BGP protocol |
| CSCek74114 | Infrastructure | ASL: Rollback was NOT able to remove ASL configuration |
| CSCek77066 | Infrastructure | SNMP query returns incorrect flash name |
| CSCin96568 | Infrastructure | FTS-7514-1: CISCO-PROCESS-MIB support for modular IOS |
| CSCin97208 | Infrastructure | Standby does not come up during switchover with slavenvram in access |
| CSCin99048 | Infrastructure | Crash seen when "class-map type inspect" or "sh class-map type inspect |
| CSCir00786 | Infrastructure | AAA authorization shouldnt be invoked when updating Boot Variables . |
| CSCsa58550 | Infrastructure | Alignment correction at ipc_process_raw_pak |
| CSCsa78886 | Infrastructure | v-access leak with pppoe session even though SSS requests v-access . |
| CSCsb14936 | Infrastructure | SNMPv3 EngineID (default value) not established correctly |
| CSCsb80841 | Infrastructure | router crashes when configuring interface range on HWIC-4ESW |
| CSCsb85983 | Infrastructure | bootflash corruption seen even with CSCei17174 fix |
| CSCsb92309 | Infrastructure | reimplementation of cache_interface_state under CSCdw09607 |
| CSCsc04397 | Infrastructure | Spurious memory access made at Fcheck_interface_state |
| CSCsc06891 | Infrastructure | no traps are sent when CF is inserted or removed. |
| CSCsc13652 | Infrastructure | SNMP: value of _LargestFree is greater than total amount of memory. |
| CSCsc13670 | Infrastructure | Rollback: backups generated are truncated at times in archive feature . |
| CSCsc33350 | Infrastructure | snmp trap link-status compulsorily becomes disable in dot1Qsubinterface |
| CSCsc44237 | Infrastructure | memory leak in client applications iterating over an empty idb list |
| CSCsc53414 | Infrastructure | IOS Low Memory Caused by SSH |
| CSCsd13491 | Infrastructure | show memory statistics history displays wrong values in processor pool |
| CSCsd23127 | Infrastructure | IPC-SP-2-LOCK IPC-SP-2-UNLOCK followed by tracebacks on SSO s/w |
| CSCsd24224 | Infrastructure | SSO: standby reloads due to config sync error atno exception crashinfo |
| CSCsd29469 | Infrastructure | Cat6000 SNMP stops responding while polling from ciscoEnhancedMemPoolMIB |
| CSCsd32923 | Infrastructure | Bus Error in Exec attempting command completion in a full command buffer |
| CSCsd36608 | Infrastructure | Multiple IPC Versioning Process instances causing memory leak |
| CSCsd37284 | Infrastructure | SP06: Unexpected exception to CPUvector 2000, PC = 0 when copy rmon cfg |
| CSCsd38693 | Infrastructure | Renaming ATA/CF file to a name ending with ... corrupts DOS File System |
| CSCsd49133 | Infrastructure | Alarms are not pouplated in ceAlarmTable - ceAlarmList is empty. |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd59610 | Infrastructure | %SYS-4-REGEXP: new engine: regexp compilation had failed. |
| CSCsd62013 | Infrastructure | Traceback on Standby RP@add_lpmapping_entry_private+74 |
| CSCsd65958 | Infrastructure | Incorrect value for ifHCInOctets, ifHCOutOctets, ifHCInUcastPkts |
| CSCsd70700 | Infrastructure | rsp crashed with TB pointing to ralib_event_card_inserted() |
| CSCsd72511 | Infrastructure | SNMPv3 community strings are sent in the clear (TACACS+ accounting) |
| CSCsd77560 | Infrastructure | snmp auth/priv users are not persisted across reload |
| CSCsd77751 | Infrastructure | IOS - SUP720 - sends empty/blank syslog messages |
| CSCsd80252 | Infrastructure | verify /md5 returns error msg %Error computing MD5 |
| CSCsd90876 | Infrastructure | Rainier:memory corruption when a ' |
| CSCse10074 | Infrastructure | MF: any traps sent to a host specified to V3 user will crash active . |
| CSCse19199 | Infrastructure | C2C1: config snmp traps and host will casue SNMP entity no access 2 mins |
| CSCse22016 | Infrastructure | MLPoATM config gets truncated and link goes down after router reload |
| CSCse42502 | Infrastructure | snmp-queue length incorrect |
| CSCse56676 | Infrastructure | Some SNMP notifications go to the wrong host |
| CSCse80032 | Infrastructure | Mediation Device cannot resync SNMP engine time after 7600 reload . |
| CSCse82855 | Infrastructure | show monitor event-trace error message prints to syslog not terminal |
| CSCse95758 | Infrastructure | Access Lists support for all CONFIG-COPY-MIB protocols under snmp-server |
| CSCse98807 | Infrastructure | Traceback, Process=SNMP Timers, %SCHED-3-STUCKMTMR during regression . |
| CSCsf00284 | Infrastructure | Event trace timestamps should be datetime no uptime by default |
| CSCsf03710 | Infrastructure | ION - Process and Mempool MIB - collapse of ion_mibs_all branch |
| CSCsf04921 | Infrastructure | 18SXF6: getnext loop condition detected on ciscoFlashFileTable . |
| CSCsf27228 | Infrastructure | Coredump is not working properly in NativeIOS |
| CSCsf32784 | Infrastructure | Need a mechanism to tell if a CF disk is bootable |
| CSCsg00673 | Infrastructure | SNMP query on Transient memory shows wrong values . |
| CSCsg04840 | Infrastructure | Fix the list of SA warnings |
| CSCsg06724 | Infrastructure | Box crashes with 100 VRF Lite Config with PIM & BGP |
| CSCsg15939 | Infrastructure | Switches crash after remove/plug in compact flash |
| CSCsg25826 | Infrastructure | CiscoFlashMib ciscoFlashPartitionName is truncating the flash name |
| CSCsg28584 | Infrastructure | show list does not display all entries; list corrupted |
| CSCsg32222 | Infrastructure | Need the support for 64 bit bit/second OID on Cat6k/7600 |
| CSCsg40016 | Infrastructure | show tech causes various system problems |
| CSCsg42072 | Infrastructure | Virtual Exec sessions not freeing memory |
| CSCsg43466 | Infrastructure | %IPC-5-INVALID: Invalid Dest Port w/ TB @ ipc_xmt_account after SSO |
| CSCsg61640 | Infrastructure | System repeatedly crashes with/without no ip address command |
| CSCsg70355 | Infrastructure | adopt new default summer-time rules from Energy Policy Act of 2005. |
| CSCsg71381 | Infrastructure | Disabling cisco-specific lsa and tty, removea all ospf trapa from conf |
| CSCsg80228 | Infrastructure | Additional byte appended to ifIndex causes SNMP trap misalignment |

| Identifier | Technology | Description |
|---|---|---|
| CSCsh23981 | Infrastructure | IPC ISSU: First message to seat 0x2070000 not found . |
| CSCsh28948 | Infrastructure | High CPU for sh run/wr mem with PTA sessions up |
| CSCsh46540 | Infrastructure | Router hangs with simultaneous format and copy operations |
| CSCsh64335 | Infrastructure | Snmp query on a directory with more than 127 char causes crash |
| CSCsh70638 | Infrastructure | Spurious memory access @ top_proc_hist_entry |
| CSCsh79371 | Infrastructure | SNMP memory leak for Modular IOS on 12.2(18)SXF6 . |
| CSCsh93041 | Infrastructure | PRE2: ifLastChange OID is increasing slightly over the time |
| CSCsh93638 | Infrastructure | High PacketLossSD values when gathering SAA data |
| CSCsi04892 | Infrastructure | unconfigure  no ip sla schedule 2  gives error message |
| CSCsi11056 | Infrastructure | Cannot configure http probe |
| CSCsi15080 | Infrastructure | RP crash when listing files by using the context-sensitive help |
| CSCsi17590 | Infrastructure | CPUHOG at process check heaps with 600 vrf configured on PE router . |
| CSCsi22502 | Infrastructure | installer imf.tar file not being zipped creates uninstallable image |
| CSCsi48665 | Infrastructure | Specify exact or prefix for SNMPv3 group to context name assoc. from CLI |
| CSCsi51014 | Infrastructure | disk access CLI freeze the router after running fsck . |
| CSCsi73444 | Infrastructure | IPC: %SIP200_MP-4-PAUSE: Non-master CPU is suspended for too long, from |
| CSCsj55691 | Infrastructure | HTTPS: crash at http_ssl_read when https url is not ready |
| CSCdy14140 | IPServices | bus error at tcp_outputpending caused by sh run and format slot att |
| CSCed28542 | IPServices | %SYS-2-INTSCHED: may_suspend at level 3 in IP NAT Ager |
| CSCed93425 | IPServices | DHCP Database fails to write to local flash. |
| CSCed95187 | IPServices | IP ID field is predictable for connectionless RST packets . |
| CSCee30364 | IPServices | ip ftp username not used after username was previously used in URI . |
| CSCee32814 | IPServices | Source port selection is predictable, should be harder to guess |
| CSCee73956 | IPServices | BTSH: TCP filtering support . |
| CSCef09586 | IPServices | CMs stuck in init(d) if DHCP ser. ip addr. overlaps with diff VRF |
| CSCef59415 | IPServices | routes still exists even after clear ip dhcp binding |
| CSCeh11675 | IPServices | NAT failures with port allocation |
| CSCeh35980 | IPServices | after unconfig & config of BGP, seeing a crash in TCP . |
| CSCeh83666 | IPServices | ip/ipnat_db.c: dereferenced pointer prev_block might be null |
| CSCeh86935 | IPServices | Multiple TCP services (incl. TACACS+) use incorrect source address . |
| CSCei27084 | IPServices | CLI on Discontiguous pools broken : hides later pools |
| CSCei93982 | IPServices | Modified ALG  classification base on src & dst port |
| CSCek12203 | IPServices | File system issues after unsuccessful FTP operation. . |
| CSCek25582 | IPServices | continuous Spurious Accesses at igmp_process_timers |
| CSCek66164 | IPServices | show command pipeline redirect into rcp crashes the router |
| CSCek68118 | IPServices | window scale option(03030001) occurs in debug ip tcp packet output . |
| CSCin78000 | IPServices | LDP session in xmit state if MPLS flapped at high traffic on L2 SUP3 |

| Identifier | Technology | Description |
|---|---|---|
| CSCsb27868 | IPServices | DHCP Relay should  unicast offer/ack on unnum ethernet sub- int |
| CSCsc12899 | IPServices | SSM Mapping configuration inside a VRF broken |
| CSCsc47919 | IPServices | VRRP does not correctly interoperate with Proxy ARP |
| CSCsc61309 | IPServices | Buffer leak in dhcpv6. |
| CSCsc78813 | IPServices | DNS reply payload does not get translated in the NAT router. |
| CSCsd23056 | IPServices | reverse telnet (tty daemon) broken by TCL feature |
| CSCsd33013 | IPServices | FHRPs fail to clear ARP entry after Duplicate IP event |
| CSCsd42600 | IPServices | %SYS-3-BAD_RESET alongwith SegV exception crash |
| CSCsd43344 | IPServices | isis-nsf info doesnt sync with standby in SSO mode . |
| CSCsd50113 | IPServices | HSRP State Change Logging Level Incorrect |
| CSCsd51530 | IPServices | autocommand-options nohangup is removed on line vty 0-4 |
| CSCsd52667 | IPServices | CLI: ip nat pool config causes cpuhog and router crash . |
| CSCsd61092 | IPServices | SSM-Mapping enabled in the vrf but not NVGEN'd |
| CSCsd69052 | IPServices | Netbios/NAT optimization |
| CSCsd80754 | IPServices | HSRP Active-Router not respond to ARP request about VIP |
| CSCsd87810 | IPServices | IOS tftp server should not differentiate between / and backslash in path |
| CSCse01124 | IPServices | HSRP groups stuck in Init state if dampening cfgd on certain interfaces |
| CSCse02028 | IPServices | Some commands fail in APPEND of FTP which uses KRON. |
| CSCse04560 | IPServices | tftp-server allows for information disclosure . |
| CSCse05106 | IPServices | sh mls netflow ip sw-installed does not show any flow with  NAT config. |
| CSCse05736 | IPServices | A router running RCP can be reloaded with a specific packet . |
| CSCse23548 | IPServices | modular ios (ION) : logging source-interface command ignored |
| CSCse51263 | IPServices | RP side console Exec process hangs deadly sometimes |
| CSCsf16715 | IPServices | TCP will leak TCBs if app closes in notification callback context |
| CSCsf27218 | IPServices | Router does not reply to TCP ECHO request |
| CSCsf33034 | IPServices | T/B tcb_isvalid+7C during bootup and when EOMPLS vc is configured. |
| CSCsg00846 | IPServices | Crash of RP blob due to a missed inetd_service_mutex unlock |
| CSCsg19598 | IPServices | SSH session hangs intermittently |
| CSCsg38013 | IPServices | ssh ipv6 client not working with ION image . |
| CSCsg39837 | IPServices | Add Transport Port Agent to allow reserving/randomly generating ports |
| CSCsg49882 | IPServices | ip ftp source-interface ip address & interface chang after write mem |
| CSCsg56926 | IPServices | no logging console not working in ION for tcp debugs |
| CSCsg59059 | IPServices | sup720 crashes when delete ip nat pool after clearing nat translations |
| CSCsg78218 | IPServices | can not remote ip rcmd mwam 0.0.0.0 mwan enable on 12.2(18)sxd7a |
| CSCsg99331 | IPServices | Show host doesn't display hostname fully for Unknown, temp entries . |
| CSCsg99600 | IPServices | Modular IOS : ip helper address 1.1.1.255 not work |
| CSCsh21505 | IPServices | ip helper address on vrf interface in ION, dhcp routed with global table |

| Identifier | Technology | Description |
|---|---|---|
| CSCsh24843 | IPServices | DHCP Relay-Agent forwarding out incorrect VLAN using IP-Unnumbered |
| CSCsh25210 | IPServices | 'ip dhcp database' may fail by running 'config replace' |
| CSCsh31939 | IPServices | c2w1:ciscoFtpClientMIB:Get & Set opration cause process deadlock & crash |
| CSCsh33430 | IPServices | Crash in hsrp_addr_hash_lookup or hsrp_addr_hash_lookup_interface |
| CSCsh36234 | IPServices | install commands fails with SCP as source . |
| CSCsh56081 | IPServices | Spanning tree of vlan-bridge is operated incorrectly |
| CSCsh58099 | IPServices | ftp process should call a registry cleanup- Message Could not register.. |
| CSCsh59375 | IPServices | Relay_vrf:dhcp ip addr not switched after smart-relay enabled . |
| CSCsh59439 | IPServices | Unable to configure same HSRP virtual MAC address on several interfaces |
| CSCsh75069 | IPServices | Input Queue Wedge with UDP Echo packets . |
| CSCsh75240 | IPServices | nat log translations syslog does not work |
| CSCsi10974 | IPServices | Error configuring dhcp option 67 |
| CSCsi29875 | IPServices | 3/27: SP: oir_rf_reload_self: icc_req_imm failed, node not booting |
| CSCsi33626 | IPServices | Tracebacks in qde_start in transport_port_agent, semaphore unitialized |
| CSCsi40766 | IPServices | H323 calls fail after router processes total of 54535 calls |
| CSCsi45840 | IPServices | ARP requests for HSRP virtual IP may fail after switchport cmd is used . |
| CSCsi51178 | IPServices | Switch crashes due to ssh session at pak_client_set_pid . |
| CSCsi77774 | IPServices | On modular IOS,Telnet on VRF int is allowed irrespective of vrf-also key |
| CSCsj07297 | IPServices | Config Sync: in no vrrp 1 preempt and standby resets |
| CSCsj09846 | IPServices | crash during bootup with ALIGN-1-FATAL:Illegal access to a low address |
| CSCsj22472 | IPServices | BGP forced deleting vrf ARP entry if BGP session is not up |
| CSCsj38828 | IPServices | Sierra:Memory Leak on HTTP Core Task during Webauth/http access |
| CSCdz80245 | LAN | SNMP: Need ifDescr output without description |
| CSCek46996 | LAN | Cwan FA-PA port need to be in promiscous mode if IP address not conf |
| CSCek65222 | LAN | vlan config produces inconsistent results |
| CSCsc69537 | LAN | GigE sub-interfaces not registered with SNMP after LC reload |
| CSCsd34855 | LAN | VTP update with a VLAN name >100 characters causes buffer overflow . |
| CSCsd94687 | LAN | sh vlans counters and SNMP counters are incosistent for subif |
| CSCse25462 | LAN | VTP password configuration should follow IOS conventions |
| CSCse40078 | LAN | VTP integer wrap |
| CSCsf25728 | LAN | Unable to session to FWSM when source-bridge ring-group is configured |
| CSCsd55300 | LegacyProtocols | DLSw ER LLC session fails to connect with SUP720 or SUP32 |
| CSCse13882 | LegacyProtocols | Show dlsw peer caused router to crash |
| CSCse17611 | LegacyProtocols | DLSw Circuits Connect outside of DLSW ER to switch with passive mapping |
| CSCei29821 | Management | cns config initial is not getting removed from startup configuration |
| CSCek36010 | Management | Need show cdp port <module> option in IOS |
| CSCse95996 | Management | PRC: config.failure recvd when attr is verbose=all, legacy CLI |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg05873 | Management | Buffer leak with SNA Focalpoint PU consuming middle buffers with NMVTs |
| CSCsg88433 | Management | IP Telephone issues seen with  Dhcp snooping and NAC posture validation |
| CSCsh79171 | Management | SNMP GetNext on cdpGlobalLastChange.0 returns error |
| CSCdy83805 | MPLS | %MPLS_TE-3-CONSISTENCY: consider replacing errmsg with buginf |
| CSCdz08851 | MPLS | FRR doesnt trigger on ethernet using RSVP HELLO |
| CSCec56047 | MPLS | TE:gtag-rrr: TSP Tunnel not up (Destination IP address not found) |
| CSCed21063 | MPLS | TE Tunnel Destination Label Missing |
| CSCed71976 | MPLS | MPLS error messages are incomplete and need improvement (TE) |
| CSCef02056 | MPLS | Inter-AS TE lsp keeps on re-signal when RSVP Policy rejects on ASBR |
| CSCef59507 | MPLS | Dead LDP session still shows up after new session established |
| CSCef87449 | MPLS | RRR LM: Admin shut handler does not preempt LSPs |
| CSCeg11894 | MPLS | MPLS VPN: Forwarding failure between CSC-PE and PE to CSC-CE link |
| CSCeg74562 | MPLS | LDP Scalability Problem with high neighbor count |
| CSCeg83614 | MPLS | Crash while signalling FRR BW-P LSP |
| CSCeh18195 | MPLS | MPLS-TE: packet loss when switching to tunnel intf after OL clears |
| CSCeh29183 | MPLS | Tracebacks and FIB messages on auto-tunnel mesh bringup |
| CSCeh32706 | MPLS | Inter-AS LSP is fail to signal after rebooting headend as ASBR box |
| CSCeh51720 | MPLS | TE LM floods link in wrong area after links area is changed in ospf |
| CSCeh53373 | MPLS | MPLS TE Inter-Area Node Protection Broken |
| CSCeh54615 | MPLS | LDP Label Mapping msg optimization problems |
| CSCeh55186 | MPLS | MPLS-TE: Pasive i/f command on broadcast links does not work properl |
| CSCeh72672 | MPLS | rainier: duplicate per-vrf aggregate labels in LFIB after SSO swtove |
| CSCei83160 | MPLS | PIM neighbor not recognised with multicast vrf tunnel. |
| CSCej00319 | MPLS | RP Crash for E2 E3 E4 E4P interaction |
| CSCej01615 | MPLS | LDP Scaling Problem with Release and Withdraw Messages |
| CSCej10404 | MPLS | BN: 10GE - remote P fails to FRR - loss >50ms |
| CSCek28918 | MPLS | BGP Peer route is NOT re-installed after clear ip route * |
| CSCek30891 | MPLS | Traffic loss during reopt for zero bw TE LSPs |
| CSCek35484 | MPLS | FRR: MP tears down protected lsp if local protection des flag rese |
| CSCsa65819 | MPLS | BGP IPv4+Labels: Make send-label unconfigurable on non MPLS images |
| CSCsa77411 | MPLS | RP crash at rrr_lm_unlock_bandwidth |
| CSCsb29168 | MPLS | FRR-MIB: protected option is not properly displayed |
| CSCsb29326 | MPLS | FRR-MIB:snmpwalk fails with cmplsFrrFacObjects |
| CSCsb52900 | MPLS | mpls forwarding table label inconsistency after switchover |
| CSCsb85903 | MPLS | R3.1 :Stdby RP Crashed @netsuper_lookup while becoming Active on SSO |
| CSCsb99035 | MPLS | MPLS-TE Tailend does not reflect Path MTU into max pkt size |
| CSCsc02825 | MPLS | 12.3 Bus Error crash due to MPLS TDP process |

| Identifier | Technology | Description |
|---|---|---|
| CSCsc14208 | MPLS | 7600: Automesh tunnels went down after changing loopback IP address |
| CSCsc40236 | MPLS | NRT: Multipath for IPv4+labels is broken when mpls ip is toggled |
| CSCsc94359 | MPLS | BGP table and CEF forwarding table have mismatched labels |
| CSCsd21449 | MPLS | MPLS-TE:No protection to primary LSP whilst reoptimising to optimal path |
| CSCsd33867 | MPLS | MPLS TE Auto-Tunnel: Primary Tunnel missing protection from N-NHOP |
| CSCsd40153 | MPLS | Rainier: label is not advertise to downstream ldp neighbor after reload |
| CSCsd43514 | MPLS | CPU stuck in 99% after clear auto-tunnel backup or shut & no shut int |
| CSCsd55004 | MPLS | FRR path gets reoptimized while in Active state |
| CSCsd87844 | MPLS | change RD cause standby PRE reset |
| CSCsd87915 | MPLS | TE tunnel goes down after SSO when refresh interval is 5000msec |
| CSCse09498 | MPLS | Primary Tunnels not being established when using Auto-Tunnel mesh |
| CSCse38446 | MPLS | NRT:snmp requests hangs when doing TE_MIB - mplsTunnelResourcePointer |
| CSCse75429 | MPLS | Sierra: LDP neighbour doesnt come UP when LDP-GR is enabled |
| CSCse93633 | MPLS | Auto-tunnel primary tunnels created to id 0.0.0.0 |
| CSCsf14018 | MPLS | sierra IOU/ION crash at vrf_sub_destroy() on config/unconfig of VRFs |
| CSCsf19418 | MPLS | sh mpls ldp graceful-restart can cause router restart |
| CSCsf98345 | MPLS | vrf-interface down cause LDP peer reset |
| CSCsg11718 | MPLS | vrf stuck in delete pending state |
| CSCsg17790 | MPLS | Large traffic drops intermittently observed on PRE3 switchover |
| CSCsg22369 | MPLS | FRR in Ready state when bak tun is down after te config toggled in IGP |
| CSCsg44555 | MPLS | 7600 MPLS TE mid-point stuck at up/down and Juniper headend up/up |
| CSCsg96651 | MPLS | %TDP-3-PTCLREAD: peer 6.6.6.6:0, read failure seen w/  VCs going down |
| CSCsh23227 | MPLS | Packets dropped on FRR backup tunnel with FA |
| CSCsh35249 | MPLS | targeted LDP convergence improvements |
| CSCsh38086 | MPLS | TE tunnels can have maximum uptime 49 days, 17 hours, 2 minutes |
| CSCsi14211 | MPLS | LDP process should optimize its cleanup of a down session |
| CSCec73297 | Multicast | PIMv6: Unicasted PIM messages dropped if arriving over a non-PIM int |
| CSCee03081 | Multicast | PIMv6: Source address for the register tunnel should be configurable |
| CSCef60452 | Multicast | possible blackout when receiving Join on RPF interface (iif) |
| CSCeh67947 | Multicast | Auto-RP group 224.0.1.40 Pruned after Assert. |
| CSCej10551 | Multicast | MIB: ciscoPimInvalidRegister trap should return src of register |
| CSCej32303 | Multicast | need to remove ip pim message-interval |
| CSCej78303 | Multicast | RP crash @ pim_tt_grange_first after CMD: no ipv6 unicast-routing |
| CSCek31478 | Multicast | ip multicast boundry cmd does not take effect after modify ACL |
| CSCek36056 | Multicast | BSRv6: CLI failure on [ipv6 pim bsr candidate bsr] + BSR is broken . |
| CSCek42421 | Multicast | One prune not processed on receiving batched join/prune message |
| CSCek46450 | Multicast | consolidate CSCek33784 and CSCdv53060 |

| Identifier | Technology | Description |
|---|---|---|
| CSCek66440 | Multicast | iprouting crash at reg_attempt_remote_call with BGP |
| CSCsa64481 | Multicast | RPF error when route is bound to serial interface |
| CSCsb85290 | Multicast | IPv6 BSR: BSM forwarding breaks with ipv6 vrf implementation |
| CSCsc29555 | Multicast | Memory Leak at pimv2_build_assert |
| CSCsc72515 | Multicast | Bidir: On becoming non-DF, downstream int not deleted from olist |
| CSCsc98828 | Multicast | PIMV6: SR flag set on RP acting as first hop |
| CSCsd13124 | Multicast | Candidate BSR does not failover immediately when bsr interface is shut . |
| CSCsd16043 | Multicast | Auto-RP for multicast may prematurely expire the group to RP mappings . |
| CSCsd17747 | Multicast | Leftover ip pim vrf register-source command cause standby RP keep reset. |
| CSCsd39528 | Multicast | Sync Damage: PIM Reg tunnels with duplicate ifindex values. |
| CSCsd42929 | Multicast | Router does not ignore MLDv1 Leave group in SSM range |
| CSCsd49955 | Multicast | RPF info created by (S,G) RPT-bit prune does not change by (S,G) join |
| CSCsd64138 | Multicast | ip multicast rpf not configurable in 12.2(18)SXF3 |
| CSCsd68993 | Multicast | Fluctuation in IPv6 mcast trffic fwdng happns with large numbr of strms |
| CSCse03637 | Multicast | PIM Dense Mode - Prune sent in error after assert is won . |
| CSCse05960 | Multicast | PIM leaking memory used for xdr messages |
| CSCse09435 | Multicast | PGM router assist on GRE causes small pool buffer leak |
| CSCse20714 | Multicast | MSDP doesnt send triggered SA for non-directly connected PIM-DM source |
| CSCse34768 | Multicast | VRF PIM neighbor lost if existing vrf mroutes exceeds route-limit value. |
| CSCse34938 | Multicast | ipv6 pim bsr border command not available on LAN sub-interfaces |
| CSCse44079 | Multicast | Multicast UDL - High CPU in IGMP Input when UDL interface down . |
| CSCse92050 | Multicast | With mis-configuration, router may reload at twheel_running |
| CSCsg24505 | Multicast | PIM-DM Assert winner does not always send prune |
| CSCsg58641 | Multicast | Traceback: SCHED-2-MESSAGE: Key (PIM Process) |
| CSCsg71344 | Multicast | PIM Join is not sent when shut/no shut is done |
| CSCsg94099 | Multicast | PIM Register not sent to RP when mcast source is connected PPPoE client |
| CSCsh58021 | Multicast | InetAddress objects in CISCO-PIM-MIB returned as strings instead of hex |
| CSCsh78277 | Multicast | Sierra: mwheel CPUhog on RPF link failure causing crash . |
| CSCsh83214 | Multicast | Named access-lists (with no matches) created when used with PIM commands |
| CSCsi03359 | Multicast | Sending extra PIM hello if the first one does not go through |
| CSCeh71577 | platform-72xx | Traceback found while loading image |
| CSCeg77503 | platform-76xx | SAA Packets do not hit the outbound service policer |
| CSCeh32595 | platform-76xx | Ping fails across atm interface after configuring routing protocols |
| CSCsa47099 | platform-76xx | IPX broke on wan link of OSM-2OC12-ATM |
| CSCsa53708 | platform-76xx | OSM crashes under stress when having to pad packets |
| CSCsa95421 | platform-76xx | OSM-1OC48-POS-SS+ drops packets |
| CSCsb64975 | platform-76xx | Rate counters are erratic for a bi-dir traffic more than 2 Gig |

| Identifier | Technology | Description |
|---|---|---|
| CSCsc25557 | platform-76xx | PORT3: Router crashed in CWAN OIR Handler in attempt to lock a semaphore |
| CSCsc73288 | platform-76xx | OSM asic error:SRIC packet data CRC error |
| CSCsd25766 | platform-76xx | OSM-1OC48-POS: APS Protect-Inactive port is receiving and fwding packets |
| CSCsd80632 | platform-76xx | 12.2(18)SXE2 ifHCInOctetssub interface traffic is not close to the main |
| CSCsd88401 | platform-76xx | input packet drop w/ gt48520 mac_rx_error at port2 on OSM-2+4GE-WAN+ |
| CSCse05336 | platform-76xx | Packet drop on OSM-2+4GE-WAN+ if sub-if is created or deleted |
| CSCse26606 | platform-76xx | packet drop occur when issuing shut/no shut on other sub-if /w OSPF |
| CSCsg21429 | platform-76xx | STM-16 interface in OSM line card flaps endlessly upon SUP switchover . |
| CSCsg40425 | platform-76xx | OSM-1OC48-POS-SI+ keeping reset due to POSLC-3-SOP . |
| CSCsg87037 | platform-76xx | ATM OSM has compatibility issue with 3rd vendor device |
| CSCsh41006 | platform-76xx | change earl reset patch-limit crash disable test cmd to a config cmd |
| CSCei76630 | PPP | PP:R3:FW2+ATM:MLPPPoA+dLFI: I/O Pool MALLOCFAIL after PORT DOWN/UP |
| CSCek26657 | PPP | Rainier:STD RP showing IPV6-STDBY-4-IDB: state mismatch messages . |
| CSCek49202 | PPP | MLP: interface in invalid state when changing group fails . |
| CSCin44386 | PPP | Multilink interface flaps after a router reload |
| CSCin86885 | PPP | vip crashes due to memory corruption on freeing mlp bundle |
| CSCsb42241 | PPP | VIP crash in ct3sw_rx_interrupt with PA-MC-2T3+ PA |
| CSCsb97950 | PPP | dLFIoATM: Packets with CLP set, get punted to RP. |
| CSCsc33562 | PPP | SNMP ifInOctets shows negative value for MLP interface |
| CSCsc37902 | PPP | Standby MSFC may experience bus error after RP_MLP-4-MISCONFIGLINK. |
| CSCsc45771 | PPP | 7500 VIP4-80 Crash with Unexpected exception,  decode vip_mlp_periodic |
| CSCsc69804 | PPP | SIP1-ChOC3:Initial packets fail with SW-MLP on SIP-200 |
| CSCsd21567 | PPP | Distributed counter statistics for UUT  is incorrect |
| CSCsd30719 | PPP | A2A: Stdby sup crashes @ mlp_remove_link . |
| CSCsd35268 | PPP | MLP: Bundle line prot down after sh/no sh with min-links config |
| CSCsd43211 | PPP | Rainier: dLFIoLL with oversubscription crashes SIP-200 on HA switchover |
| CSCsd72854 | PPP | ISIS over MLPPP fails after reboot . |
| CSCse11678 | PPP | SIP: Ping fails after removal of primary link from multilink bundle. |
| CSCse20150 | PPP | SIP1-CT3:SW-MLP: all intf are going down w/46 byte pkt size @LR traffic |
| CSCse91675 | PPP | SWMLP: all intf are going down w/46 byte pkt size 8links/bundles@LR trfc |
| CSCsf10497 | PPP | MLPPP bundle across the SPAs are not configrable |
| CSCsf25712 | PPP | Sip-200 CPU1 crash @ blt_pak_holdq_peek |
| CSCsg02881 | PPP | MLP:  Bandwidth of down MLP group should be sum of member bandwidths |
| CSCsg11708 | PPP | Receive adjacency & process switching of pkts on mlp if after switchover |
| CSCsg25664 | PPP | dLIFoMLPPPoATM PA: Corrupted PC crash PR |
| CSCsg35429 | PPP | CLI:Spurious Memory access at ppp_ncp_cstate . |
| CSCsi48550 | PPP | dMLP: account lost_frags&  rx discards as bundle intf input error |

| Identifier | Technology | Description |
|---|---|---|
| CSCec26696 | QoS | RSVP shows wrong allocated bw in show ip rsvp interface |
| CSCec80902 | QoS | Router crashes with Bus Error at 0xFD011147 |
| CSCec85835 | QoS | RSVP treats compressed flows as non-conformant |
| CSCed54330 | QoS | WFQ on virtual-template causes allocation error and tracebacks |
| CSCed79634 | QoS | police percent conversions are incorrect in 2nd and 3rd lvl policies |
| CSCee13430 | QoS | Crash observed when reconfiguring channel-group |
| CSCee36050 | QoS | VIP crash when re-use channel group with set service policy |
| CSCee47275 | QoS | card resets due to [no] fair-queue cleanup loops |
| CSCee56112 | QoS | Show Policy interface input/output should not display all. |
| CSCee66909 | QoS | ct3 spa: qos configs should be blocked on multilink member links |
| CSCee68344 | QoS | GE-WAN card crashes in /enqueue/process-policymap_msg/policymap_hash |
| CSCee69260 | QoS | FIFO queueing with QoS service-policy |
| CSCef21601 | QoS | ResvConfirm dropped when non-RSVP hops exist along a calls path |
| CSCef25953 | QoS | dwred statistics are not updated in show policy-map int output |
| CSCef44588 | QoS | Info: Illegal normal burst size seen with default config |
| CSCef46134 | QoS | CPUHOG at CEF MQC IPC Background on SIP-600 on remove/apply qos |
| CSCef63607 | QoS | Crashes seen during boot if ATM WIC is installed & NAT on int config |
| CSCef66517 | QoS | packet drop on flexwan when traffic shaping |
| CSCef91275 | QoS | RSVP: policy does not retry outbound request after failure |
| CSCeg25493 | QoS | VIP Bus error crash in get_same_id_actiongroup |
| CSCeg30179 | QoS | NRT: crash @ hqflayer_update() |
| CSCeg33229 | QoS | VIP crash when service policy removed from MFR int with traffic |
| CSCeh31441 | QoS | Flexwan module powercycles with shaping+dLFIoATM |
| CSCeh54083 | QoS | random-detect aggregate cmd not working for virtual-template |
| CSCeh82893 | QoS | PP:R3:SIP400:QOS: LLQ+police drop rate counters are broken |
| CSCeh84740 | QoS | VIP crash on RPR+ switchover with qos config and high load traffic |
| CSCei09171 | QoS | PP:R3:SIP-200: %C7600_SIP200_MP-4-PAUSE @ fibidb_handle_delete |
| CSCei10181 | QoS | PP:R3:FW+MLP+MLFR:MALLOCFAIL for LLQ+CBWFQ to hit the LC crash |
| CSCei16615 | QoS | Neighber crash at avl_get_first when shut/no shut tunnel on LSP-head |
| CSCei24965 | QoS | PP:R3: Block qos policy with bandwidth guarantee of > 100% |
| CSCei65865 | QoS | Policy doesnt send modified path to downstream with refresh reductio |
| CSCei67700 | QoS | frde failed to match control packets on fr over AToM |
| CSCej09368 | QoS | Abnormal queue depth for time and byte based WRED on ETH over AToM |
| CSCej77367 | QoS | RP crash at hqf_check_vc_layertype during qos testing |
| CSCek05730 | QoS | Bus error crash at mlp_fastswitch_les. |
| CSCek25851 | QoS | Rainier:PWAN2: Router crash @hqf_police_update on attaching qos poli |
| CSCek29478 | QoS | MPLS TE tunnel fails with path option Loose as first hop |

| Identifier | Technology | Description |
|---|---|---|
| CSCek34117 | QoS | SIP1+ATM(OC3 SPA): Crashed at hqf_walk_and_police_inline() . |
| CSCek37011 | QoS | Rainier:SIP-200:LC crash @hqf_dp_fifo_cleanup on rem HQoS child pol |
| CSCek43669 | QoS | defaultclass input policy not work for non-queue class for sip1 atm |
| CSCek44025 | QoS | Hierarchy is not collapsed when FRF.12 is configured |
| CSCek63384 | QoS | Service-Policy is Lost When the Multilink Interface is Reset . |
| CSCin72437 | QoS | MQC: Concurrent access crashes the Flexwan during switchover |
| CSCin86096 | QoS | Classification matching on IPv6 acl fails |
| CSCin96590 | QoS | RSP: VIP crash @free_wred_stats on rpr+ s/o w/ traffic w/mlp-qos |
| CSCin96938 | QoS | Spurious access at no_vc_backpressure |
| CSCsa68661 | QoS | LC crashes when service-policy is configured on channelized interface |
| CSCsa80132 | QoS | RSVP reservation across  secondary link torn down after 1 minute |
| CSCsb25607 | QoS | dLFIoFR: all lp pkts dropped on oversubscribed mixed traffic |
| CSCsb32141 | QoS | Router reloads when admitting an RSVP flow |
| CSCsb36818 | QoS | Service policies lost on interface bw reconfiguration |
| CSCsb40118 | QoS | Unable to reserve more than 99% of bandwidth |
| CSCsc00993 | QoS | Lower tx-ring-limit for ATM VCs with higher SCR when QoS is enabled |
| CSCsc35609 | QoS | Crash in rvsp tail-end while shuting down egress interface on mid |
| CSCsc39917 | QoS | show policy-map interface shows default bandwidth for class-default |
| CSCsc43751 | QoS | RR & Auth interop issue: test for Integrity obj in bundle msg too strict |
| CSCsc62327 | QoS | Bad RSVP MD5 Authentication Messages when many topology changes |
| CSCsc90843 | QoS | Crash in HQF when deleting service-policy |
| CSCsc93633 | QoS | Software bus error crash on 7206VXR w/12.3(14)T3 w/ NBAR configured |
| CSCsc95511 | QoS | Bus error crash at hqf_scheduler_info_init |
| CSCsc98510 | QoS | Ehanced Flexwan reloads with VRF/MLPPP/QoS |
| CSCsd09892 | QoS | no fair-queue causing VIP crash . |
| CSCsd17641 | QoS | SIP-400 QOS: after changing hier. policy, the policy no longer attaches |
| CSCsd37025 | QoS | CPUHOG and crash when removing nbar policy-map |
| CSCsd47863 | QoS | Refresh are not sent downstream after change in path with RR+policy |
| CSCsd56696 | QoS | A2A: FR Adaptive shaping is not accurate . |
| CSCsd68445 | QoS | Unable to attach the new hierarchical service policy onto the sub-intf . |
| CSCsd71119 | QoS | ALL ATM PVC DOWN IN FLEXWAN WITH PA-A3-OC3 AND OAM |
| CSCsd71131 | QoS | dLFIoLL + QoS : service policy is suspended after clear int mul1 |
| CSCsd76528 | QoS | Queues not released after deletion of mtch vlan for HQoS policies . |
| CSCsd95712 | QoS | VIP4-80 with local switching and QoS crashing |
| CSCse02510 | QoS | Crash with ALIGN-1-FATAL at hqf_process_wfq_command |
| CSCse17960 | QoS | Address Error crash with tcp retransmit to ATM VC with qos |
| CSCse22161 | QoS | RP pool Memory corruption SXF4 - checkheaps_process/validblock crash |

| Identifier | Technology | Description |
|---|---|---|
| CSCse94388 | QoS | SIP200 crash at dlfi_do_fragment on HQF with priority . |
| CSCsf11353 | QoS | Autobahn:FW2 kept crash at hqf_dp_set_blt_quantum and dlfi_inform_config |
| CSCsf20194 | QoS | SIP-200 crashes after OIR when both input and out policy attached to MFR |
| CSCsf27085 | QoS | SIP200 CPU1 crash@hqf_sip1_work_with_callback on removing priorit class |
| CSCsh46565 | QoS | PWAN2 HQoS(LLQ): shape ave rate is not applied . |
| CSCsh65322 | QoS | ATM output packet drops on 7600 with Enhanced FlexWAN and PA-A3-OC3SMI . |
| CSCsh76895 | QoS | Multiple conform and voillet action allowed under single classmap . |
| CSCsi01422 | QoS | Hierarchical Frame-Relay QoS does not work . |
| CSCsi05251 | QoS | bus error crash at get_rateinterval_from_service_policy at subint delete |
| CSCea46927 | Routing | ISIS-NSF: Cautiously refresh neighbor adjacency on RR reception |
| CSCed06329 | Routing | BGP-v6: Version number churns when multipath configured on BGP-v6 |
| CSCed17879 | Routing | adtvertise ipv4 routes across ipv6 BGP peers not working |
| CSCed23406 | Routing | Redistributed routes stuck in RIP database permanently |
| CSCed84633 | Routing | support for intf option in distribute-list under address-family. . |
| CSCed87897 | Routing | sh ip route missed default gateway after ip default-net command |
| CSCee01688 | Routing | NAS crashes at ip2access_add_acl_item() while running stress test |
| CSCee35050 | Routing | %OSPF-4-NORTRID not correct with multiple vrfs using same IP |
| CSCee40207 | Routing | Memory leak in BGP Open Process After SSO RP Switchover |
| CSCee43724 | Routing | CsC BGP ipv4+label not consistent with e-bgp next-hop change |
| CSCee50452 | Routing | RRI: static routes removed from config when peer disconnects |
| CSCef50427 | Routing | System crashed when show ip bgp XX. |
| CSCef59924 | Routing | ISIS: rtr. crash at isis_free_next_hop_parent_list |
| CSCef70161 | Routing | vrf peers with same policy fall into different update-group . |
| CSCef93058 | Routing | ARP req was send with delay when each VRF uses same dest IP |
| CSCef97738 | Routing | BGP/MVPN: incorrect update-source is passed from BGP to MVPN |
| CSCeg03019 | Routing | cef not working between different tunnels . |
| CSCeg13748 | Routing | Ping loss to HSRP vip address of a VRF interface on sup720 |
| CSCeg16631 | Routing | CSCee32557 breaks RIP distribute-list w/ VRF interface |
| CSCeg52659 | Routing | BGP route may not get withdrawn under rare condition |
| CSCeg57155 | Routing | BGP: network statement prefix is not originated when auto-summary on . |
| CSCeg58039 | Routing | BGP: changing the max-paths value may cause a crash . |
| CSCeg85719 | Routing | IPHC: UDP frames from MWR1900 or RPM-XF may be discarded |
| CSCeh09588 | Routing | 300 second traffic loss with 100 OSPF neighbor after SSO switchover |
| CSCeh31691 | Routing | CWAN-MFI: Pos interfaces do not work with PPP encap |
| CSCeh35659 | Routing | 4 port gig per-interface ip bgp fast-external-fallover permit . |
| CSCeh41328 | Routing | Multi-topology transition deletes IPv6 routes from RT |
| CSCeh41598 | Routing | Router reload on rip_process_mgd_timers |

| Identifier | Technology | Description |
|---|---|---|
| CSCeh62512 | Routing | all ping failed after SSO switchover on all the vrf interfaces |
| CSCeh66944 | Routing | mdt safi with NSF is not working |
| CSCeh80535 | Routing | IPv6 PING packet dropped at 6PE router |
| CSCeh92012 | Routing | OSPF did not redistribute route expectedly |
| CSCei04409 | Routing | Crash in CBTS while using show adjacency int filter command on vip |
| CSCei04683 | Routing | PP:R3:IPV6:Default ISIS Route Generated from L1/L2 to L2 Router |
| CSCei06089 | Routing | Conditional default-originate with route-map does not work in 28S3 |
| CSCei12603 | Routing | 30ms traffic loss on reoptimzation while BW change over TE tunnel |
| CSCei25214 | Routing | router crash @registry fastcase_expection w/ ip cef dist command |
| CSCei25442 | Routing | BGP MVPN - sanitise notification to PIM database |
| CSCei25454 | Routing | BGP: The BGP IPv4 MDT table may receive RD type 2 prefixes |
| CSCei29944 | Routing | RP crashes at bgp_get_msg_count while sho ip bgp summ |
| CSCei32930 | Routing | EBGP+label : soft-reconfig inbound broken |
| CSCei45669 | Routing | OSPF router may fail to flush its self-originated LSA |
| CSCei53226 | Routing | BGP: fix updgrps for non private-as peers with remove-private-as |
| CSCei58655 | Routing | ISIS not aging version of LSP in isis local rib |
| CSCei59309 | Routing | Crash in  iprouting_set_ndb_last_rdb() |
| CSCei60544 | Routing | BGP: redistribute connected routes missing from bgp after removing IGP |
| CSCei62049 | Routing | SPD classification removed from fast path |
| CSCei65252 | Routing | IOS forwarding packets for non-routable addresses in the 0.0.0.0/7 |
| CSCei65553 | Routing | OSPF must accept LSID with a mix of 0/1s in the host portion |
| CSCei67996 | Routing | Unbalanced load-sharing tsp tunnel when morethan 1 tunnel is applied |
| CSCei75828 | Routing | CPUHOG when 4000 IPv6 VLANs |
| CSCei83720 | Routing | DMVPN:NHRP hold timer refreshed every 5000msec on Spoke router |
| CSCei93768 | Routing | check heaps CHUNKBADMAGIC crash at BGP Router when remove dmzlink ba . |
| CSCej00946 | Routing | mVPN: remote PE tunnel interface wont show up when SSM configed . |
| CSCej31343 | Routing | Active RP crash at fib_upd_record_is_delete when no ip vrf vpn1 |
| CSCej35288 | Routing | Null IDB in ipsendnet -process traceback when failover from PRE2A-B |
| CSCej36831 | Routing | VRF-lite/leaking:50% loss to local IP |
| CSCej42345 | Routing | Creating SVI Triggers ARP for the Static NAT IP addresses. |
| CSCej48262 | Routing | The session exceeded MTU counter has NOT  incremented correctly for |
| CSCej76134 | Routing | spurious memory access in isis_area_address_match |
| CSCek24782 | Routing | 5400XM reloads unexpectedly with stress with AAA holding excess mem |
| CSCek32139 | Routing | SSO : Spurious access at ip_spd_fib_punt_feature_check |
| CSCek32244 | Routing | Not all routes locally generated with auto-summary enabled |
| CSCek35039 | Routing | next-hop isnt matched in the route-map . |
| CSCek35061 | Routing | Disassociate VRF from a MPLS interface crashes the router |

| Identifier | Technology | Description |
|---|---|---|
| CSCek36037 | Routing | BGP: Initial keepalive algorithm should be more aggressive |
| CSCek38025 | Routing | MDT interoperability with old image is not working . |
| CSCek38584 | Routing | ISIS IP route is del/add/del when interface shutdown |
| CSCek39048 | Routing | Modular IOS: default distribute-list route-map crash router . |
| CSCek39701 | Routing | ospf adj is not maintained over p2p after swithover |
| CSCek41338 | Routing | CLI: rsp router reloads while configuring under template conf mode |
| CSCek42585 | Routing | BGP Does not establish with Third Party boxes after Link Flap |
| CSCek45564 | Routing | iprouting crash with corrupted block on mpath config change |
| CSCek47667 | Routing | clear bgp ipv6 unicast * does not work . |
| CSCek47888 | Routing | TE LSPs torn down and resignalled after ISIS process restart |
| CSCek48274 | Routing | clear ip bgp soft in  may not delete all the BGP prefix |
| CSCek58880 | Routing | RP crashed in ospf_rrr_find_telink/ospf_intfc_command |
| CSCek62005 | Routing | ip prefix list deletes lists before sending notif (causing rtr crash |
| CSCek62848 | Routing | BGP does not notify PIM of RD type 1 mdt safi updates |
| CSCek65928 | Routing | redundancy config-sync failures prc for router isis ipv6 cmd |
| CSCek69969 | Routing | router crash when show ip bgp internal |
| CSCek76093 | Routing | CLNS neighbor is still formed on router after isis protocol disabled |
| CSCek77849 | Routing | bgp aggregate-address results in high BGP Router process utilization |
| CSCin85894 | Routing | Reflexive acl when used as ext. acl gives T/bks & crashes with std. |
| CSCsa55567 | Routing | Crash during show xdr multicast-group (xdr_mcast_display_all) |
| CSCsa68864 | Routing | Loadsharing over 2 equal cost sham-links is not working |
| CSCsa69518 | Routing | MVPN : MDT update is sent with RD 0:0 |
| CSCsa72510 | Routing | %COMMON_FIB-DFC1-4-CHAIN_REMOVE_INCONS1 seen on reset of mod 2 |
| CSCsa78050 | Routing | Alignment errors in internet_enqueue |
| CSCsa82134 | Routing | router reload when there are over 64 equal cost next-hops for IPv6 |
| CSCsa82564 | Routing | MVPN: Repeated Bus Error on 30S1 |
| CSCsa86801 | Routing | Traceback messages seen at ipigrp2_route_map_inform. |
| CSCsa87034 | Routing | clear bgp ipv4 unicast  command does not clear Routing table |
| CSCsa87473 | Routing | BGP:MPLS/VPN: After reload PE missing prefixes from RR. |
| CSCsa88766 | Routing | PRP crash due to BGP |
| CSCsa90843 | Routing | ARP is not resolved properly |
| CSCsa91499 | Routing | Suprious Access seen from fib_table_flush |
| CSCsa97101 | Routing | FIBNULLIDB in create path due to race condition |
| CSCsb01157 | Routing | CEF Scanner runs when new vaccess interface is created |
| CSCsb06829 | Routing | Loadinfo freed without unregistering dependency if path weight >127 |
| CSCsb08994 | Routing | test ip command returns ambiguous command error. |
| CSCsb09709 | Routing | removing bgp with ipv6 address family causes crash (watchdog timeout) |

| Identifier | Technology | Description |
|---|---|---|
| CSCsb09852 | Routing | BGP: pathless nets not freed when updgrp members are out of sync |
| CSCsb12089 | Routing | CEF: RF proceeds to standby hot before standby is fully synced |
| CSCsb12896 | Routing | SSO:routes in a vrf is not synced in CEF between active and standby |
| CSCsb24535 | Routing | clear ip bgp update-group [ip address] clears all the bgp peers |
| CSCsb28300 | Routing | Standby stuck in stanby cold bulk after loadversion |
| CSCsb36755 | Routing | BGP does not delete multi-path route when receiving worse metric UPDATE |
| CSCsb40115 | Routing | BGP: Failed to find expected # of multipath entries |
| CSCsb44220 | Routing | ipfast needs to retry openning the ipc port in the background |
| CSCsb47281 | Routing | Stdby stuck in cold bulk after LV |
| CSCsb50606 | Routing | Leak in dead process due to TCBs from BGP active connections |
| CSCsb54823 | Routing | BGP: prefixes temp advertised despite prefix-list ORF . |
| CSCsb63652 | Routing | bgp aggregate-address results in high BGP Router process utilization . |
| CSCsb64858 | Routing | reset during icmp redirect packet generation/determination |
| CSCsb66121 | Routing | MPLS TE tunnel: export netflow pak wth IP TTL=0 |
| CSCsb75669 | Routing | BGP: restore next-hop-self command for eBGP peers |
| CSCsb77733 | Routing | Failed to ping  the IPv6 loopback interface due to IPv6-CEF-Drop |
| CSCsb79895 | Routing | RIP protocol with MD5 authentication fails |
| CSCsb83521 | Routing | %SCHED-3-STUCKMTMR - Process= IPC LC Port Opener after SSO |
| CSCsb86987 | Routing | Traceback from bgp_ipv4_mcast_lookup() after reload |
| CSCsb89043 | Routing | %ALIGN-3-SPURIOUS access made at adj_ios_update_fixup_and_macstr. |
| CSCsb89900 | Routing | ISIS: tracebacks %SYS-3-MGDTIMER: Parent is a leaf, set_exptime_internal |
| CSCsb92705 | Routing | password command not displayed in show bgp template peer-session command |
| CSCsb96034 | Routing | Traffic down for too long after SSO switchover . |
| CSCsc00378 | Routing | export map is not taking affect dynamically when PE-CE runs ospf |
| CSCsc16611 | Routing | 7304 router crashes due to watchdog timeout |
| CSCsc30197 | Routing | Router crashes at Config command router isis with traceback |
| CSCsc37212 | Routing | ISIS: Redistributed routes might not be advertised if interface flaps |
| CSCsc41457 | Routing | NHRP: Registration cache entries do not override no-socket mappings |
| CSCsc41694 | Routing | router hangs while unconfiguring the CLI  no router bgp <No> |
| CSCsc43989 | Routing | CEF adjacency inconsistent with NHRP cache entry |
| CSCsc49231 | Routing | Traceback seen with SYS-3-MGDTIMER Running timer, init, NHRP |
| CSCsc59027 | Routing | mem leak in CEF IPC Background process |
| CSCsc59089 | Routing | BGP: updates missing if route-refresh received while updates on OutQ |
| CSCsc67367 | Routing | set ip next-hop in-vrf not working with import maps |
| CSCsc72090 | Routing | EIGRP doesn't honor interface IP MTU when sending packets |
| CSCsc74229 | Routing | VPN routes get deleted from the BGP table though counter shows otherwise |
| CSCsc75426 | Routing | Crash when BGP sends update with bad attribute . |

| Identifier | Technology | Description |
|---|---|---|
| CSCsc76327 | Routing | EIGRP PE-CE: Constant route-flap with a redistributed VRF-static-route |
| CSCsc83742 | Routing | BGP MAXPFX Sylog message does not include VRF tableid info |
| CSCsc83821 | Routing | ISIS: TLV 237 not found in database when isis metric is configured |
| CSCsc98835 | Routing | CPUHOG when access-list is modified causes OSPF and BGP session drops . |
| CSCsd00028 | Routing | OSPF: spurious access in ospf_generate_trap |
| CSCsd03021 | Routing | 360K internal routes will produce CPUHOG messages and tracebacks . |
| CSCsd04128 | Routing | Packets drop after reloading master switch and getting back to a stack |
| CSCsd04810 | Routing | Route pointing towards an interface where IP is not enabled but ISIS is. |
| CSCsd11019 | Routing | Rainier:After RPR-Plus switchover standby RP crashes |
| CSCsd12046 | Routing | Receiving foreign packets from the network |
| CSCsd15749 | Routing | SoO-tagged prefixes sent when SoO configured on peer group . |
| CSCsd28214 | Routing | RIP watchdog timeout crash on flapping links |
| CSCsd32373 | Routing | BGP does not flag multipath correctly, causing loadbalancing issues . |
| CSCsd33445 | Routing | SYS-3-MGDTIMER: Running timer message for NHRP |
| CSCsd41237 | Routing | vrf import map is not working . |
| CSCsd50101 | Routing | NRT:  Intermittent crashes going to issu loadversion |
| CSCsd51309 | Routing | SUP720  crashes every time after disabling auto-tunnel mesh feature |
| CSCsd52225 | Routing | BGP soft-reconfiguration keeps the old next-hop |
| CSCsd53402 | Routing | ABR delets OSPF summary route for 5sec after DR is changed |
| CSCsd59023 | Routing | RP Arping for adjacent next-hop bringing up PTA sessions with AAA . |
| CSCsd60687 | Routing | T/B untyped_dqueue_match_its seen during RPR switchover |
| CSCsd63038 | Routing | MVPN: BGP session for IPv4 MDT between any two PEs never comes up |
| CSCsd64173 | Routing | Bus error crash IPV6 due to OSPF summary prefix command |
| CSCsd66372 | Routing | BGP: router crashes at bgp_scan_walker |
| CSCsd67591 | Routing | OSPF: crash while modifying route-map . |
| CSCsd67768 | Routing | 1200 BGP peer sessions with 10/30 keepalive/holdtime values flap often. |
| CSCsd72747 | Routing | nssa summary to null0 disappears after 'clear ip ro *' |
| CSCsd73245 | Routing | IPRT-3-PATHIDX: Bad path pointer of 0 message is reported. |
| CSCsd74189 | Routing | show ip bgp vpnv4 vrf NAME community-list NAME gives error mesg. |
| CSCsd74396 | Routing | eigrp authenticaion fails with md5 enabled |
| CSCsd75574 | Routing | VIP crashed with IOBUS Error Interrupt Status register 0x4 |
| CSCsd76419 | Routing | IPv6 ND and CEF do not match |
| CSCsd76832 | Routing | NRT: Output interface not available with ip_route_and_transmit traceback |
| CSCsd81600 | Routing | OSPF Stub-links should advertise LSInfinity when max-metric configured |
| CSCsd82809 | Routing | Can't add a static ipv6 route on an interface with ipv6 unnumbered |
| CSCsd84489 | Routing | Crash in ospf_add_all_stub_routes on topology change |
| CSCsd88685 | Routing | ISIS overload-bit on startup does not work with RPR+/SSO fail-over |

| Identifier | Technology | Description |
|---|---|---|
| CSCsd89569 | Routing | sh ip int brief output - Any interface listed with OK? msg |
| CSCsd94133 | Routing | sh ip cef exact route for vrf and 6PE ipv6 shows no oce |
| CSCsd98686 | Routing | %XDR-6-CLIENTISSUBADTXTFM: Failed to xmit_transform message . |
| CSCsd98763 | Routing | MRAI betwen PE and CE defaults to 30 seconds |
| CSCsd99760 | Routing | After iprouting.iosproc Process Restart Routing table not updated |
| CSCse04220 | Routing | Clearing IPv6 BGP sessions can cause crash . |
| CSCse05031 | Routing | BGP conditional default-originate with route-map doesnot work correctly |
| CSCse07118 | Routing | OSPF: crash while using the transmit-interface command . |
| CSCse10102 | Routing | BGP Update-group: inconsistent error mesg. when EIGRP is PE-CE |
| CSCse10683 | Routing | BGP Route-refresh double-counted |
| CSCse18445 | Routing | BGP4-MIB should not send trap for IPv6 BGP peer. |
| CSCse19783 | Routing | ip cef load-sharing configuration can't be removed |
| CSCse26515 | Routing | DR does not flood back LSA on receipt of LSA from DROTHER router |
| CSCse26682 | Routing | Ping failure with isatap configuration |
| CSCse26921 | Routing | BGP route is not updated with newly configured route-target |
| CSCse26941 | Routing | Bus error configuring cef table output-chain build favor convergence-spe |
| CSCse29589 | Routing | c18xx tracebacks when trying to send NHRP registration |
| CSCse30000 | Routing | ATT-bit control for dual-homed L1 ISIS |
| CSCse34050 | Routing | ISIS keep advertizing passive interface, even after doing shutdown |
| CSCse40346 | Routing | NRT:Router Crashed with tracebacks while testing isis_ldp |
| CSCse41174 | Routing | NRT: GSR router crashed at ospf_send_one_paced_update during l2tun test |
| CSCse41484 | Routing | DMVPN / VPN-SPA / few GRE packets not encrypted when negotiating the SAs |
| CSCse44052 | Routing | Crash when config IPv6 interface distribute list |
| CSCse49697 | Routing | can not disable bgp nexthop trigger tracking NHAT |
| CSCse51804 | Routing | DMVPN tunnels not stable; keeps flapping |
| CSCse54241 | Routing | ISIS - LSP purge not sent for DIS removal |
| CSCse57232 | Routing | Display lsa throttle timer in sh ip ospf by default |
| CSCse61025 | Routing | ip http auth aaa is not needed for Authproxy to work |
| CSCse64565 | Routing | OSPF passive-interface default pb when converting switchport to L3 |
| CSCse66181 | Routing | BGP PMTUD cannot be turned off for peer group |
| CSCse67487 | Routing | Autobhan76: Router Crashed in the unconfig section. |
| CSCse69162 | Routing | Multi-topology ISIS breaks CLNS routing |
| CSCse72792 | Routing | OSPF: neighbor cmd rejected if VL configured |
| CSCse74643 | Routing | ISIS metric maximum is missing under sub-interface |
| CSCse77758 | Routing | No IPv6 unicast-routing command disables ipv6 cef . |
| CSCse78454 | Routing | ipv6 ospfv3 cfg lost from interface on restart iprouting.iosproc . |
| CSCse82584 | Routing | OSPF does not remove MAXAGE LSAs |

| Identifier | Technology | Description |
|---|---|---|
| CSCse85383 | Routing | OSPFv3: Restructure link-state request list (CSCsd03021) |
| CSCse86806 | Routing | 'clear ip bgp soft out' failed to send defaul-originate |
| CSCse87859 | Routing | no service udp-small-server does not block IPv6 udp port 7 (echo) |
| CSCse89119 | Routing | OSPF discard route (Null0) is disappeared from RIB when AD is changed |
| CSCse90843 | Routing | Fib entries not freed - remain in deleted state |
| CSCse91962 | Routing | prefix stays in BGP table with RD 0:0 even after vrf's RD is configured |
| CSCse97513 | Routing | BGP session to a Third Party router does not come up after reload |
| CSCsf00171 | Routing | summary route not flushed from ospf database |
| CSCsf02935 | Routing | Router Crash due to Ospf Sham link and BGP redistribution |
| CSCsf05579 | Routing | ISIS passive-interface default problem in IOS 12.2(18)SXF |
| CSCsf11980 | Routing | NHRP: Crash w/ OSPF, DMVPN @ max_proto_mtu nhrp_send_resolution_request |
| CSCsf15429 | Routing | 7304 Router Crash @ fr_bq_proc continuous loop FR Broadcast Output |
| CSCsf20947 | Routing | BGP 'neighbor default-originate' advertisement ignored after link flap. |
| CSCsf26043 | Routing | Cat6k Selective Packet Discard not classify ISIS at high-priority |
| CSCsf32449 | Routing | Sup720 MVPN PE - Tunnel does not come back up after reload . |
| CSCsf99057 | Routing | JQL: OSPF Stub-router should work with SSO/RPR-Plus if NSF is disabled |
| CSCsg02387 | Routing | Timeout response with SNMP over IPV6 phase II |
| CSCsg03483 | Routing | FIB-4-FIBCBLK: Missing cef table for tableid 1 during route update XDR e |
| CSCsg07742 | Routing | ip vrf sitemap soo requires bounce when removing/re-adding |
| CSCsg14026 | Routing | Routers/Switches forward traffic destined to Class E Addresses |
| CSCsg16748 | Routing | ABR deletes OSPF type 3 LSA after it received max-aged type 2 LSA |
| CSCsg17977 | Routing | Non-master CPU is suspended for too long @ mtrie_leaf_insert |
| CSCsg21418 | Routing | Bus error related to CLNS fast switching |
| CSCsg26492 | Routing | Error: can not find acl. Abort - msg when removing permit entry in ACL . |
| CSCsg28497 | Routing | MT isis adj flaps during GSR RP FO causing prolonged traffic loss |
| CSCsg29248 | Routing | OSPF: summary-address cmd can create stale  LSA . |
| CSCsg29498 | Routing | adj trace stores pointer not value = Segmentation Fault |
| CSCsg33571 | Routing | Add prefix option under router xxx vrf process distribute-list options |
| CSCsg34030 | Routing | show bgp ipv6 unicast longer-prefixes not showing expected output |
| CSCsg40507 | Routing | SIERRA:ISIS/BFD session doesnt come up after changing ip-addr of interf |
| CSCsg42246 | Routing | CPUHOG in IP Background, and router reload . |
| CSCsg42488 | Routing | Juniper - Cisco PE incorrect extended community for OSPF |
| CSCsg43140 | Routing | Switch may crash due to bgp over vpn . |
| CSCsg45637 | Routing | Traceback occurs while accessing bgp_vpnv4_lookup_prefix . |
| CSCsg46366 | Routing | OSPF NSSA LSA forwarding address set even when P bit wil be clear. |
| CSCsg46638 | Routing | BGP does not send withdraw when distribute-list is configured |
| CSCsg49166 | Routing | EIGRP fails to converge with 1100 neighbors on FR point to point PVCs |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg52336 | Routing | Crash at ospf_flush_area_summary_lsa after 'no ip vrf' of unassigned vrf |
| CSCsg52887 | Routing | SegV at ctunnel_oqueue when 'no ctunnel destination' on one side |
| CSCsg55209 | Routing | BGP paths increase, with same prefix and next-hop under soft-reconfig . |
| CSCsg55591 | Routing | MPLS VPN Local label not allocated/programmed for sourced BGP network |
| CSCsg59699 | Routing | OSPFv3 autocost gives interfaces the wrong cost sometimes . |
| CSCsg65298 | Routing | OSPF: connected network learnt via ospf after interface shutdown #2 |
| CSCsg65625 | Routing | flo_isp: Assertion failed: fib_instance_can_be_used |
| CSCsg66635 | Routing | TE metric becomes invalid after reboot . |
| CSCsg71797 | Routing | bgp bestpath as-path multipath-relax - command crashes Supervisor card |
| CSCsg74898 | Routing | IPHC: Juniper interop: Timestamp on the RTP Packet not to update |
| CSCsg78246 | Routing | ISIS Wide redistribution metric shows incorrectly on local table |
| CSCsg83723 | Routing | %COMMON_FIB-3-DEPENDENCY_WALK: error message seen |
| CSCsg84690 | Routing | ospf: default route with a bad mask may not get installed . |
| CSCsg85846 | Routing | PE does not flush VPN Summary LSAs when redist is cleared |
| CSCsg95101 | Routing | ALIGN-3-SPURIOUS: Spurious memory access |
| CSCsh02161 | Routing | BGP vpnv4 route reflector not withdrawn redistributing prefix . |
| CSCsh11482 | Routing | incorrect link-local next-hop for prefixes from update-group 'leader' |
| CSCsh13291 | Routing | Traceback@xdr_rp_disable_slot due to XDR keepalive timeout |
| CSCsh13542 | Routing | LOOPPAK detected for UDP ECHO Back packets |
| CSCsh14457 | Routing | SIERRA: supw crashes @ ospf_nbr_find_retrans_block with OSPF/BFD |
| CSCsh15066 | Routing | VRF has 2 ospf process, when one process is removed the router crashed |
| CSCsh15489 | Routing | OSM-1CHOC12 FR tcp header-compression needs reload to take effect |
| CSCsh19852 | Routing | ospfv3: stale network LSA after DR interface goes down ; also v2 problem |
| CSCsh20140 | Routing | OSPF: ispf traceback in chunk_destroy . |
| CSCsh23176 | Routing | Router crashes @ rip_timer_process . |
| CSCsh27931 | Routing | Switch crash when tunnels are shut |
| CSCsh38228 | Routing | uRPF w/exception ACL not logging deny log ACEs in interrupt path |
| CSCsh41234 | Routing | Standby router keeps reloading with SRA image |
| CSCsh42565 | Routing | TE tunnel does not come up on ospf non-broadcast network type . |
| CSCsh51559 | Routing | Spurious access made at bgp_vpn_afmodify_walker |
| CSCsh53926 | Routing | Bus error crash at add_path - ispf . |
| CSCsh55768 | Routing | Catalyst 3550 SVI packet buffers leaked . |
| CSCsh57652 | Routing | RIP accepts update before hold down timer expires. |
| CSCsh57795 | Routing | Removing 1 RIP neighbor removes all neighbors |
| CSCsh59495 | Routing | BGP non-exist-map statement incorrectly stored as exist-map. |
| CSCsh61119 | Routing | High CPU due to ARP refresh triggered by Serial interface flap |
| CSCsh63785 | Routing | NRT:MPLS-TE tunnel down after switchover |

| Identifier | Technology | Description |
|---|---|---|
| CSCsh66406 | Routing | BGP VPN4 has stale routes after executing maximum routes 50 80 in vrf . |
| CSCsh67160 | Routing | CEF consistency checkers go offline after sso switchover |
| CSCsh67709 | Routing | BGP: 'redistribute connected' triggered only by shut/no shut local intf |
| CSCsh68376 | Routing | Routes learned from CBB route reflector didn't get refreshed . |
| CSCsh80008 | Routing | BGP: soft reconfiguration inbound and neighbor weight has no effect |
| CSCsh81289 | Routing | DFC earl adj vlan incorrect, sceompls vcs disposition fails after bootup |
| CSCsh87119 | Routing | Suppress OSPF-6-ZERO_BANDWIDTH, when interface is down |
| CSCsh92854 | Routing | output bytes not incrementing correctly in 122.SB3. |
| CSCsi03434 | Routing | Memory leak @ ospf_redist_work_enqueue |
| CSCsi06948 | Routing | Bus error when issuing BGP dampening related commands . |
| CSCsi11438 | Routing | OSPF does not remove maxage LSAs and age goes to bigger than 16 bit |
| CSCsi14346 | Routing | EIGRP: neighbor command missing in VRF. |
| CSCsi23719 | Routing | 'no isis protocol shutdown' on a sub-interface enables 'clns routing' |
| CSCsi35541 | Routing | CPUHOG and T/B seen after clearing ospf routes |
| CSCsi41944 | Routing | Virtual Exec CPUHOG |
| CSCsi45422 | Routing | iprouting.iosproc process reloads when making changes to static routes |
| CSCsi49948 | Routing | MDT prefixes are not installed and sent out on iprouting restart . |
| CSCsi57971 | Routing | ISIS does not advertise prefix of passive interface |
| CSCsi58867 | Routing | CPUHOG After show ip route static or show ip route connected |
| CSCsi60103 | Routing | IPv6 OIR PA Name Clash enhancements |
| CSCsi60240 | Routing | prefix-list change not processed for redistribute route-map correctly. |
| CSCsi62559 | Routing | SPD classifies OSPF IP Precedence 0 as priority . |
| CSCsi65922 | Routing | Cannot unshut BGP neighbor once it is shutdown |
| CSCsi68819 | Routing | Prefixes are moved to non-fwd tree after delete when RPR is configured |
| CSCsi68882 | Routing | Crash@ network_redist after executing no router eigrp . . |
| CSCsi86386 | Routing | clear ip bgp * soft in does not work for inbound route-map for ip4 label |
| CSCuk49694 | Routing | 6PE: Ignoring label update from peer |
| CSCuk52253 | Routing | IPv6 static route missing tag argument |
| CSCuk54191 | Routing | MP-iBGP routes not installed in VRF RIB |
| CSCuk54781 | Routing | ICMPv6 Packet too big does not account for label stack |
| CSCuk55579 | Routing | CEFv6 inconsistencies found after a HA Switchover |
| CSCuk58462 | Routing | Routes are not filtered even when route-map rule sets deny the rule |
| CSCuk58481 | Routing | Crash in fib_path_list_ifnums_compare() |
| CSCuk60585 | Routing | ISO-IGRP: Crash may occur when nv-gening redistribution into iso-igr |
| CSCuk60910 | Routing | IPHC:invalid TCP header may cause memory corruption & reload |
| CSCdu83050 | Security | ssh needs source-address |
| CSCdz34708 | Security | GRE : tunnel path-mtu-discovery doesnt copy DF bit to GRE+IP header |

| Identifier | Technology | Description |
|---|---|---|
| CSCed68627 | Security | Dynamic spoke to spoke tunnel fails to come up with dual-DMVPN |
| CSCed73942 | Security | IDBs for tunnel interfaces are not reused |
| CSCei70222 | Security | VAM2+: epa_get_blk_buffer FAILED after overnight stress test |
| CSCei85164 | Security | OCSP fails when timezone is configured |
| CSCej43220 | Security | 7200 Dynamic VTI tunnels take 10 seconds to come up |
| CSCek30711 | Security | te-mib caseMIB_TE_cli_get_set_get fail due to CLI return nullset |
| CSCek30748 | Security | Router reloads when config tunnel protection ipsec profile vpnprof |
| CSCek56735 | Security | IPV6IP tunnel with VRF does not switch data packets. . |
| CSCek73041 | Security | SSH:Connection closed message not seen after the retry prompts |
| CSCin48676 | Security | Quatro:SSH V2:Switch reloads @ checkSurrender due to V2 session |
| CSCsb47257 | Security | bus error crash @ pki_add_to_obj_list |
| CSCsb54378 | Security | watchdog timeout crash when starting ssh session from the router . |
| CSCsb62045 | Security | scp connection fails with error: unexpected filename: |
| CSCsb74409 | Security | IOS ssh client blocks Virtual Exec / SSH Process |
| CSCsc23816 | Security | clear crpto sa peer A.B.C.D command does not reset the tunnel |
| CSCsc30451 | Security | Some VTI interfaces remain down despite ike & ipsec sa created |
| CSCsc72722 | Security | CBAC - firewall resets TCP idle timer upon receiving invalid TCP packets |
| CSCsd00341 | Security | GRE tunnel CEF switches via invaild adj when sequence-datagrams configd |
| CSCsd30932 | Security | CLI: router reload on bad refcount error during CA trust point config |
| CSCsd38247 | Security | CLI: default keepalive command causes router crash . |
| CSCsd76601 | Security | Resuming SSH Session Fails After Other Session Has Been Disconnected . |
| CSCsd77758 | Security | packet loss from tag2ip with double GRE encapsulation using tunnel vrf |
| CSCsd80510 | Security | Default tunnel bandwidth and delay are not reasonable values. step 1 |
| CSCsd92405 | Security | router crashed by repeated SSL connection with malformed finished messag |
| CSCse03277 | Security | VTI: VTI tunnel does not come up after remove/add tunnel configuration |
| CSCse11457 | Security | show crypto ca timers  shows static output |
| CSCse12154 | Security | Bus error crash after executing secure copy (scp) |
| CSCse22153 | Security | Rainier:%COMMON_FIB-STDBY-2-IF_NUMBER_ILLEGAL message on stby. . |
| CSCse29545 | Security | Crypto pki trustpoint loses ip-address command upon reload |
| CSCse40423 | Security | With ATM, tunnel interfaces do not ping until a shut-noshut is done . |
| CSCse62462 | Security | MFI - VRF Tunnel packet is sent unlabeled |
| CSCse69736 | Security | Update tunnel default bandwidth and delay |
| CSCse79611 | Security | SSH source-interface command not working |
| CSCse93597 | Security | RSA keys not replicated via SSO redundancy to standby |
| CSCsf25722 | Security | software forced reload after executing secure copy (scp) |
| CSCsf30150 | Security | GRE: Tunnel interface should go down when tunnel source interface up/dwn |
| CSCsf96592 | Security | midchain loop restart requires input_if swap and all-encap bytecount |

| Identifier | Technology | Description |
|---|---|---|
| CSCsg10671 | Security | No message when CA re-enrollment fails |
| CSCsg47462 | Security | Address error crash at tunnel_ep_addr_compare |
| CSCsg62226 | Security | IPSEC: crash@ ace_reverse_map while checking the traffic flow with ipsec |
| CSCsh25172 | Security | scp can't be used to copy large files |
| CSCsh26382 | Security | Ipsec SAs getting deleted for AH+ESP Transform set |
| CSCsh41459 | Security | The router crashes, when removing/adding VRFs |
| CSCsh56320 | Security | Memory Leak when executing sh crypto ipsec or sh crypto session |
| CSCsh66935 | Security | Crash in avl_get_next_threaded on deconfiging 100 tunnels/vrfs |
| CSCsh75224 | Security | RP crashes due to stack overflow with ssh |
| CSCsi21930 | Security | mplsTunnelPerfHCPackets value mismatch CLI ouput |
| CSCsb46223 | Voice | Bus error crash at Tcl_DStringAppend |
| CSCek31227 | VPDN | Router Crashed while testing Voluntary L2TP Tunneling |
| CSCef71011 | WAN | Trans/Bridging: All pings fail when serial(atm-dxi) in use. |
| CSCeh35068 | WAN | Frame-relay:CEF adjacency is not established until flap the interfac |
| CSCeh41080 | WAN | PP:FW2:MIV:Marking does not work,either basic or with policer. |
| CSCek27504 | WAN | NTP crash during show runn after deletion of NTP ref-peer |
| CSCek42041 | WAN | Inconsistent DTR pulsing |
| CSCek45604 | WAN | All OSM modules on the router crashes with FR qos configs . |
| CSCsa72748 | WAN | router crash due to watchdog timeout on frame relay broadcast |
| CSCsb44267 | WAN | bus error crash when forwarding IPX over GRE |
| CSCsb86675 | WAN | Multicast Packets are forwarded out on down PVC on ATM Bundle |
| CSCsc50986 | WAN | NTP unsynchronizes when packets out of order at STEP |
| CSCsc66187 | WAN | %CWPA-3-IPCSENDFAIL: Failed to send IPC message for loveletter . |
| CSCsd19880 | WAN | ATM pvc does not come up with new style legacy command |
| CSCsd59878 | WAN | Packet switching on FlexWAN stops for 15 secs during an SSO switchover . |
| CSCse55004 | WAN | NTP clients wont associate |
| CSCse87862 | WAN | SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe regn with SNMP IM by driver |
| CSCse95146 | WAN | Sup720 with cross module etherchannel duplicates all packets |
| CSCsi33554 | WAN | Connected net for virtual-template is not created in vrf routing table |
| CSCsi70727 | WAN | LFI Not Working with Cisco<-->Cisco Encapsulation on Frame-Relay |